Oracle® Secure Global Desktop

Platform Support and Release Notes for Version 4.62

E23646-01
November 2011

Oracle® Secure Global Desktop: Platform Support and Release Notes for Version 4.62

Abstract

This document describes the new and changed features for Oracle Secure Global Desktop 4.62. It also lists what is supported and the known bugs and issues.

Table of Contents

Preface

The *Oracle Secure Global Desktop Platform Support and Release Notes for Version 4.62* provide information about the system requirements and support, and the new features and changes, for this version of Oracle Secure Global Desktop (SGD). This document is written for system administrators.

1. Audience

This document is intended for new users of SGD. It is assumed that readers are familiar with Web technologies and have a general understanding of Windows and UNIX platforms.

2. Document Organization

The document is organized as follows:

- Chapter 1, *New Features and Changes* describes the new features and changes for this version of Secure Global Desktop.
- Chapter 2, *System Requirements and Support* includes details of the system requirements and supported platforms for this version of Secure Global Desktop.
- Chapter 3, *Known Issues, Bug Fixes, and Documentation Issues* contains information about known issues, bug fixes, and documentation issues for this version of Secure Global Desktop.

3. Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

4. Related Documents

The documentation for this product is available at:

http://www.oracle.com/technetwork/documentation/sgd-193668.html

For additional information, see the following manuals:

- *Oracle Secure Global Desktop 4.6 Administration Guide*
- *Oracle Secure Global Desktop 4.6 Installation Guide*
- *Oracle Secure Global Desktop 4.6 Gateway Administration Guide*
- *Oracle Secure Global Desktop 4.6 User Guide*

5. Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1. New Features and Changes

This chapter describes the new features and changes in Oracle Secure Global Desktop (SGD) versions 4.60, and 4.50.

1. New Features in Version 4.60

This section describes the features that are new in the SGD version 4.60 release.

1.1. Automatic Recovery After Array Failover

This release supports automatic recovery of an array after failover.

In version 4.50, the original primary server did not rejoin the array after failover and you had to manually recreate the original array formation. In this release, the original array formation is recreated automatically by default.

The process of failover, followed by recovery of the original array formation is called *array resilience*. The new Global Settings, Resilience tab in the SGD Administration Console is used to configure array resilience.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about array resilience.

1.2. Dynamic Launch

Dynamic launch is the term used to describe runtime changes that are applied when users start applications. Typically, the runtime changes enable users to select the application server that runs the application, or to choose the application that is started, or both.

The following new object types have been introduced for dynamic launch:

- Dynamic application servers
- Dynamic applications

The `tarantella object new_host` command has been extended to include support for creating dynamic application server objects.

The following commands have been introduced to create and configure dynamic application objects:

- `tarantella object new_dynamicapp`
- `tarantella object add_mapping`
- `tarantella object remove_mapping`

Client overrides have been extended to support dynamic launch features, such as password caching.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about how to configure dynamic launch.

1.3. Active Directory and LDAP Enhancements

Version 4.6 contains significant enhancements and performance improvements for integrating SGD with Active Directory and Lightweight Directory Access Protocol (LDAP) directories.

For Active Directory and LDAP directories, there are enhancements to how SGD handles password expiry. SGD can now be configured to do the following:

- Display a warning message on the webtop, telling the user that their password is about to expire
- Deny authentication and force the user to reset their password at the next log in

For Active Directory, the following enhancements can be used to tune how SGD discovers LDAP information:

- **Site awareness** – If SGD detects, or is configured with, site information, it queries only the Active Directory servers appropriate for the site.
- **Whitelist** – A whitelist is a list of global catalog servers that are *always* used for LDAP queries. Only those servers that are included in the whitelist can used for LDAP queries.
- **Blacklist** – A blacklist is a list of Active Directory servers that are *never* used for LDAP queries. Blacklists override any other configuration such as sites or whitelists.
- **Search only global catalog** – SGD searches for user information only from the global catalog instead of contacting a domain controller.

Other configuration settings are also provided for tuning connections to Active Directory and LDAP directories.

In previous releases, Active Directory or LDAP configuration settings applied globally. In this release, *service objects* have been introduced to provide more flexibility. A service object is a group of directory services configuration settings that can be applied to one or more LDAP directories or Active Directory forests. You can create and manage service objects on the Global Settings, Service Objects tab in the SGD Administration Console, or with the new `tarantella service` command. The Administration Console only enables you to configure the commonly-used settings.

Most of the command-line options for filtering user logins and tuning LDAP group searches have changed. It is also now possible to filter (deny or allow) user logins based on the membership of LDAP groups.

Options have been added to the `tarantella cache` command to improve the caching of LDAP group data. The `--populate` option adds LDAP group and LDAP group membership information to the cache. The `--refresh` option updates the cache with the current membership of LDAP groups.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for details of how to use service objects to tune directory services configuration.

1.4. Dynamic Drive Mapping

This release includes support for “hot plugging” of removable storage devices during a user session. This feature is called *dynamic drive mapping*.

Dynamic drive mapping is enabled by default for an SGD server. To disable or enable dynamic drive mapping, use the Dynamic Drive Mapping (`--array-dyndevice`) attribute.

The `native-cdm-config` file used to configure the available drives on UNIX® and Linux platform client devices now includes a list of default system locations which are monitored for removable drives. Users upgrading from earlier versions of SGD must rename their existing `native-cdm-config` file before connecting to the upgraded SGD server. A new `native-cdm-config` file containing the default system locations is created automatically when the SGD Client first connects to the upgraded server. Any custom configuration present in the backed up file can be merged with the new file.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about array resilience.

1.5. Windows Client Drive Mapping

In this release, client drive mapping (CDM) for Windows applications is implemented using Remote Desktop Protocol (RDP) instead of the Server Message Block (SMB) protocol. As a result, you do not need to install the SGD Enhancement Module on the Windows application server to provide CDM services. Application server drive letters are no longer displayed when using CDM for Windows applications.

Windows CDM is now enabled separately from CDM for UNIX platform applications. Two new attributes, Windows Client Drive Mapping (`--array-windowscdm`) and Unix Client Drive Mapping (`--array-unixcdm`) have been introduced for this. The attributes apply to all SGD servers in the array.

A restart of CDM is not required when configuring CDM for Windows applications. Consequently, the `tarantella start cdm` and `tarantella stop cdm` commands are now only applicable to CDM for UNIX platform applications.

Ports used for connections between SGD servers and application servers have changed as follows:

- TCP Port 139 was previously used for all CDM services. This port is now only used for CDM for UNIX platform applications.
- TCP Port 137 is no longer used by SGD.

The following CDM attributes have been deprecated for this release:

- Client Drive Mapping (`--array-cdm`)
- Windows Internet Name Service (WINS) (`--array-cdm-wins`)
- Fallback Drive Search (`--array-cdm-fallbackdrive`)

1.6. New Attributes for Configuring Windows Applications

New attributes have been introduced to configure Windows applications. The attributes correspond to command options for the SGD Remote Desktop Client, also known as the `ttatsc` command.

Previously, `ttatsc` command options were configured using the Arguments for Protocol (`--protoargs`) attribute of the Windows application object. This method is still supported for those `ttatsc` options that do not have a corresponding Windows application attribute.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about the new attributes and their equivalent `ttatsc` command options.

1.7. New Attributes for Application Load Balancing

New application server object attributes for filtering application servers have been introduced.

The Maximum Count (`--maxcount`) attribute specifies the maximum number of SGD application sessions that can be run concurrently on the application server.

The User Assignment (`--userassign`) attribute specifies the users that can run applications on the application server.

These attributes can be used individually or together to control the application servers that can run an application for a user.

1.8. 32-Bit Color Support for Windows Applications

SGD now supports 32-bit color depths in a Windows Terminal Server session.

32-bit color is available on Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7 platforms. The client device must be capable of displaying 32-bit color.

1.9. Allow SSH Downgrade Attribute

In previous releases, to display X applications through SGD using an SSH connection, you had to enable X11 forwarding.

The Allow SSH Downgrade (`--allowsshdowngrade`) attribute for X application objects has been introduced, to enable the display of X applications when X11 forwarding is not available.

If this attribute is enabled and X11 forwarding is not working or not configured, SGD attempts to display the application using a regular unsecured X11 connection. Depending on your configuration, users might be prompted to accept the downgrade.

1.10. Span Multiple Monitors Profile Setting

A new client profile setting has been added, to provide support for displaying X applications in kiosk mode on a multihead or dual head monitor.

Enabling the Span Multiple Monitors (Kiosk Mode) setting causes the display to be spanned across all monitors.

2. New Features in Version 4.50

This section describes the features that are new in the SGD version 4.50 release.

2.1. Introducing the SGD Gateway

This release introduces the Oracle Secure Global Desktop Gateway (SGD Gateway).

The SGD Gateway is a proxy server designed to be deployed in front of an SGD array in a demilitarized zone (DMZ). This enables the SGD array to be located on the internal network of an organization. Additionally, all connections can be authenticated in the DMZ before any connections are made to the SGD servers in the array.

Using the SGD Gateway is an alternative to running your SGD servers with firewall traversal, also called firewall forwarding.

The SGD Gateway manages load balancing of Hypertext Transfer Protocol (HTTP) connections, so you do not need to use the JavaServer Pages™ (JSP™) technology load balancing page included with SGD.

The SGD Gateway software is included with the SGD distribution.

Instructions on how to install, configure, and use the SGD Gateway are included in the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide*. This document also includes details of supported platforms.

2.1.1. Installing the SGD Gateway

To install the SGD Gateway, click the Install the Oracle Secure Global Desktop Gateway link on the SGD web server Welcome Page and follow the instructions on the screen.

By default, the SGD Gateway is installed in the `/opt/SUNWsgdg` directory on the SGD Gateway host.

2.1.2. Architecture of the SGD Gateway

The SGD Gateway consists of the following components:

- **Routing proxy**. A Java™ technology-based application that routes Adaptive Internet Protocol (AIP) data connections to an SGD server.

  Keystores in the routing proxy contain the certificates and private keys used to secure connections for the SGD Gateway.

  The routing proxy uses routing tokens to manage AIP connections. A routing token is a signed, encrypted message that identifies the origin and destination SGD server for a route.

- **Reverse proxy.** An Apache web server, configured to operate in reverse proxy mode.

  The reverse proxy also performs load balancing of HTTP connections.

See the Appendix A of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* for more details about the architecture and features of the SGD Gateway.

2.1.3. Commands for the SGD Gateway

New commands have been introduced for the SGD Gateway, as follows:

- `gateway` – The `gateway` command is used to control and configure the SGD Gateway.

  You run this command on the SGD Gateway host.

- `tarantella gateway` – The `tarantella gateway` command is used to register gateways for use by an SGD array.

  You run this command on the SGD array.

A new attribute, `--security-gateway`, configures which client connections to an SGD array use the SGD Gateway.

See Appendix B of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide;* for more details about these command-line changes.

2.2. Application-Level Device Configuration

This release enables application-level device configuration. For Windows applications, SGD Administrators can configure CDM and printing settings.

CDM and printing configuration for Windows application objects overrides settings configured for user profile, organizational unit, and organization objects. The order of precedence is: Windows application, user profile, organizational unit, organization.

For CDM on all platforms, the access rights for a mapped client drive are shown in brackets after the drive name: (rw) means read-write access, (ro) means read only access. For example, in Windows desktop sessions access rights are displayed in file save dialogs and in the My Computer window.

2.3. Array Failover

This release includes a new feature called *array failover*. When array failover is enabled for an SGD array, the array repairs itself automatically following the loss of the primary server.

In array failover, a secondary server in the array is upgraded automatically to become the primary server.

Array failover is disabled by default for an SGD array. To enable array failover for an SGD array, run the following command on any SGD server in the array:

```
$ tarantella config edit --array-failoverenabled 1
```

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about configuring array failover for an SGD array.

2.4. Seamless Windows Local Window Hierarchy

A new attribute SWM Local Window Hierarchy (`--swmopts`) for Windows applications has been introduced for compatibility with some Borland applications. The attribute is only effective for applications having a Window Type setting of Seamless Window. Use this attribute if you are having problems with minimizing and maximizing the application window from the task bar.

A corresponding command option `-swmopts` has been added for the SGD Terminal Services Client program, `ttatsc`.

2.5. German Language Support

This release includes support for the German language.

The webtop, the Administration Console, and the SGD Client are available in German. The documentation is not translated into German.

2.6. Support for Novell eDirectory

Novell eDirectory version 8.8 or later is now supported as an LDAP directory server.

By default, Novell eDirectory requires that all simple LDAP binds that contain a password must be encrypted. To use simple binds with a password for SGD, you must do either of the following:

- Configure SGD to use secure connections to eDirectory by using `ldaps://` Uniform Resource Locators (URLs)
- Configure the LDAP group object in eDirectory and disable Transport Layer Security (TLS) for simple binds

3. Changes in Version 4.60

This section describes the changes since the SGD version 4.50 release.

3.1. Improved Clock Synchronization Reporting for Arrays

Array join operations are now only permitted if the clock on the server joining the array is in synchronization with the other servers in the array. If the time difference is more than one minute, the array join operation fails.

The `tarantella status` command now reports any clock synchronization issues for an array. The `--byserver` option of this command displays the clock setting on each server in the array.

If the clocks in the array are out of synchronization, a warning message is displayed on the Secure Global Desktop Servers tab of the Administration Console.

Use Network Time Protocol (NTP) software or the `rdate` command to ensure the clocks on all SGD hosts are synchronized.

3.2. Citrix ICA Protocol Not Available for Windows Applications

In this release, Citrix ICA is not supported as a connection protocol for Windows applications. Windows applications are now configured to use the Microsoft RDP protocol by default.

As an alternative, you can configure the Citrix ICA Client as an X application object.

3.3. Application Start Time Shown on the Webtop

The webtop link for a running application now shows the time and date when the application was started.

3.4. User Session Idle Timeout Attribute

The User Session Idle Timeout (`--webtop-session-idle-timeout`) attribute can now be configured using the Global Settings, Communication tab of the Administration Console. Previously, this attribute was only configurable from the command line.

The command line name for this attribute has changed, from `--tarantella-config-array-webtopsessionidletimeout`.

3.5. Web Page Security Improvements

In this release, the following security improvements have been made for SGD web pages.

- Autocompletion of user input can be disabled for the SGD login page and the Administration Console login page. Disabling autocomplete prevents browser caching of sensitive data, such as user names and password.

  To disable autocomplete, edit the `/opt/tarantella/webserver/tomcat/`*`tomcat-version`*`/conf/web.xml` file and change the value of the `disableloginautocomplete` parameter to `true`. This parameter is `false` by default. Restart the SGD web server after making changes.

- Cross-frame scripting (XFS) vulnerabilities have been fixed. XFS is sometimes used to attempt to steal user credentials.

  This change means that users can only access the SGD login page if JavaScript™ software is enabled in their browser. If JavaScript is not enabled, access is denied and a warning message is shown.

  

  Note

  For Internet Explorer users with JavaScript enabled, this warning message might be displayed briefly before the login page is displayed.

- If secure connections are being used, user session cookies are now marked as secure. This prevents transmission of the cookie over a non-secure connection.

- Directory indexes are disabled by default for the SGD web server. This change enhances security, as users cannot browse the directories on the SGD web server.

3.6. Support for Arabic and Hebrew Keyboards

This release adds support for Arabic and Hebrew keyboards.

Keymap files for Arabic (`xarabic.txt`) and Hebrew (`xhebrew.txt`) are included in the `/opt/tarantella/etc/data/keymaps` directory on the SGD server.

3.7. Input Method for UNIX Platform Applications

By default, SGD now runs an Input Method (IM) for UNIX platform applications for all locales except C and POSIX.

In previous releases, SGD ran an IM only for Japanese, Korean, and Chinese locales.

3.8. UNIX Audio and SGD Enhancement Module Version

To use audio for X applications, Linux and UNIX application servers must be running version 4.6 of the SGD Enhancement Module. UNIX audio services might not work correctly if the versions of SGD and SGD Enhancement Module are different.

Instructions for upgrading the SGD Enhancement Module are included in the *Oracle Secure Global Desktop 4.6 Installation Guide*.

3.9. DNS Name Warning Message

For commands where the Domain Name System (DNS) name of an SGD server must be specified, such as `tarantella array join`, a warning message is shown if the fully-qualified DNS name is not used.

For best results, always use fully-qualified DNS names.

3.10. Changes to Syslog Message Format

The SyslogSink log handler now includes the “SSGD” identifier string in messages that are recorded using `syslog`. Previously, the string “Secure Global Desktop” was used.

3.11. New Default PDF Printer Driver for Windows Applications

The default printer driver used for Portable Document Format (PDF) printing from Windows application servers is now HP Color LaserJet 2800 Series PS. This change was made to provide support for Windows 7 and Windows Server 2008 application servers.

In previous releases, the default PDF printer driver was HP Color LaserJet 8500 PS. If you are upgrading from an installation that uses this printer driver, SGD is reconfigured automatically to use the new default printer driver. If you are upgrading from an installation where you have configured SGD to use a different printer driver, your existing configuration is preserved on upgrade. If you are using using Windows Server 2003, Windows Vista, or Windows XP application servers, the new default printer driver results in the PDF printer not being mapped.

3.12. Changes to tarantella start and tarantella stop Commands

The `--force` option has been deprecated for the `tarantella start` and `tarantella stop` commands.

3.13. New Name for SGD Terminal Services Client

The SGD Terminal Services Client, also known as the `ttatsc` command, has been renamed. The new name is SGD Remote Desktop Client.

The new name is used in the Administration Console.

3.14. Secure SOAP Connections No Longer Required

In this release, there is no longer a requirement to secure SOAP connections from the webtop when you enable secure connections for an SGD server. The `tarantella security enable` command does not secure the SOAP connections automatically, as in previous releases.

This is due to a change in how listener events are handled by the SGD server.

4. Changes in Version 4.50

This section describes the changes since the SGD version 4.41 release.

4.1. Option to Resume Printing from My Desktop

If a user logs in to My Desktop and they have paused print jobs, a message now displays in the browser window which enables the user to resume printing.

4.2. Changes to the tarantella security enable Command

The `tarantella security enable` command now includes a `--firewalltraversal` option. This option enables you to choose whether or not to enable firewall traversal when you secure an SGD server.

If you do not specify this option, firewall traversal is enabled by default.

Note

SGD servers configured for firewall traversal cannot be used with the SGD Gateway.

The following example secures the SGD server using the specified SSL certificate and private key. Firewall traversal is not enabled for the SGD server.

```
# tarantella security enable \
--certfile /opt/certs/cert \
--keyfile /opt/keys/key \
--firewalltraversal off
```

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more detailed information about this command option.

4.3. Web Services Changes

The `ITarantellaWebtopSession` web service includes a new operation, `endMultiViewSession`.

The `endMultiViewSession` operation ends a user session and logs out the user. All views of the user session are ended.

Note

A *view* of a user session is created when you join an existing user session. For example, when you log in to the Administration Console and the SGD webtop from the same client device.

You use the `endMultiViewSession` operation as follows:

```
endMultiViewSession(sessionCookie);
```

where `sessionCookie` is the user session cookie.

4.4. Kiosk Mode Escape Attribute

For Windows applications and X applications running in kiosk mode, the Kiosk Mode Escape (`--allowkioskescape`) attribute for enabling a pull-down header is now configurable using the Administration Console. The attribute is available on the Presentation tab for the application object.

In previous releases, this attribute was only configurable from the command line.

4.5. Support for Evince Document Viewer

Evince Document Viewer is now supported for PDF printing on Linux client platforms.

4.6. New -remoteaudio Option For SGD Terminal Services Client

In this release, a new option (`-remoteaudio`) has been introduced for the SGD Terminal Services Client. The SGD Terminal Services Client, also known as `ttatsc`, is a client program that handles the connection between the SGD server and a Windows Terminal Server.

The `-remoteaudio` option configures whether audio is sent from the terminal server. Using this option has the same effect as the “Leave at remote computer” sound setting for a Microsoft Windows Remote Desktop connection.

For example, to leave audio at the remote server for a Windows XP desktop session, configure the Arguments for Protocol (`--protoargs`) attribute of the Windows application object as follows.

```
-console -remoteaudio
```

Note

The `-console` option is not required if the application server platform supports at least RDP version 6.

4.7. Administration Console Configuration Parameter for DNS Lookups

In this release, a new deployment descriptor parameter has been introduced to configure the class of DNS lookups used by the Administration Console.

By default, SGD uses a query class of ANY for DNS lookups. Some firewall configurations might block this class of DNS lookups. This can lead to problems, for example when configuring Active Directory authentication using the Administration Console.

To configure the Administration Console to use a query class of IN for all DNS lookups, edit the deployment descriptor for the Administration Console web application. The deployment descriptor is the following file: `/opt/tarantella/webserver/tomcat/version/sgdadmin/WEB-INF/web.xml`

In this file, set the `sgd.naming.dns.in_class_only` parameter to `true`.

```
<context-param>
    <param-name>sgd.naming.dns.in_class_only</param-name>
    <param-value>true</param-value>
</context-param>
```

Restart the SGD server to enable any changes you make to the `web.xml` file.

Chapter 2. System Requirements and Support

This chapter includes details of the system requirements and supported platforms for Oracle Secure Global Desktop (SGD) versions 4.60, 4.61, and 4.62.

1. SGD Server Requirements and Support

This section describes the supported platforms and requirements for SGD servers.

1.1. Hardware Requirements for SGD

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact an Oracle sales office.

The requirements for a server hosting SGD can be calculated based on the *total* of the following:

- What is needed to install and run SGD
- What is needed for each user that logs in to SGD on the host and runs applications

The following are the requirements for installing and running SGD:

- 2 gigabytes of free disk space
- 2 gigabyte of random-access memory (RAM)
- 1 gigahertz processor
- Network interface card (NIC)

This is *in addition to* what is required for the operating system itself and assumes the server is used only for SGD.

The following are the requirements to support users who log in to SGD and run applications:

- Minimum 50 megabytes for each user
- 50 megahertz for each user

Caution

The actual central processing unit (CPU) and memory requirements can vary significantly, depending on the applications used.

1.2. Supported Installation Platforms for SGD

The following table lists the supported installation platforms for SGD.

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	At least Oracle Solaris 10 10/09 Trusted Extensions at least Oracle Solaris 10 10/09
Oracle Solaris on x86 platforms	At least Oracle Solaris 10 10/09 Trusted Extensions at least Oracle Solaris 10 10/09

Operating System	Supported Versions
Red Hat Enterprise Linux (32-bit and 64-bit)	5.5
Oracle Enterprise Linux (32-bit and 64-bit)	5.5

1.2.1. Operating System Modifications

You might have to make some operating system modifications. Without these modifications, SGD might not install properly or operate correctly.

1.2.1.1. 5250 and 3270 Applications

The `libXm.so.3` library is required to support 5250 and 3270 applications. This library is available in the OpenMotif 2.2 package.

1.2.1.2. Oracle Solaris 10

You must install at least the End User Oracle Solaris distribution to get the libraries required by SGD. If you do not, SGD does not install.

The TCP Fusion feature of Oracle Solaris 10 can cause problems with some local socket connections used by SGD. Disable the TCP Fusion feature before you install SGD, as follows:

1. Add the following line at the bottom of the `/etc/system` file.

```
set ip:do_tcp_fusion = 0x0
```

2. Reboot the server.

1.2.1.3. Red Hat Enterprise Linux and Oracle Enterprise Linux

The default `/etc/hosts` file for Red Hat Enterprise Linux and Oracle Enterprise Linux contains a single entry, which incorrectly maps the host name of the SGD host to the local loopback address, `127.0.0.1`.

Edit the `/etc/hosts` file to remove this mapping, and add a new entry that maps the name of the SGD host to the network Internet Protocol (IP) address of the SGD host. The SGD host name must not be mapped to the local loopback IP address.

1.2.2. Virtualization Support

The supported installation platforms for SGD are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

Installation in zones is supported for Oracle Solaris 10. SGD can be installed either in the global zone, or in one or more non-global zones. Installation in both the global zone and a non-global zone is *not supported*.

On Oracle Solaris 10 Trusted Extensions platforms, you must install SGD in a labeled zone. Do not install SGD in the global zone.

1.2.3. Retirements to Supported SGD Installation Platforms

The following table shows the SGD installation platforms that have been retired.

SGD Version	Platforms No Longer Supported
4.60	OpenSolaris (all versions)

SGD Version	Platforms No Longer Supported
	Red Hat Enterprise Linux 5.0 to 5.4 Solaris 10 OS up to, and including, Solaris 10 5/09 SUSE Linux Enterprise Server 10
4.50	Solaris 8 OS Solaris 9 OS Red Hat Enterprise Linux 4 Fedora Linux 8 SUSE Linux Enterprise Server 9

1.3. Supported Upgrade Paths

Upgrades to version 4.62 of SGD are only supported from the following versions:

- Oracle Secure Global Desktop Software version 4.61
- Oracle Secure Global Desktop Software version 4.60
- Sun Secure Global Desktop Software version 4.50

If you want to upgrade from any other version of SGD, contact Oracle Support.

1.4. Java Technology Version

The following table shows the JDK™ versions included with SGD.

SGD Version	JDK Version
4.62	1.6.0_29
4.61	1.6.0_24
4.60	1.6.0_21
4.50	1.6.0_13
4.41	1.6.0_05

1.5. Required Users and Privileges

To install SGD, you must have superuser (root) privileges.

The system must have `ttaserv` and `ttasys` users and a `ttaserv` group before you can install SGD.

The `ttasys` user owns all the files and processes used by the SGD server. The `ttaserv` user owns all the files and processes used by the SGD web server.

The SGD server does not require superuser (root) privileges to run. The SGD server starts as the root user and then downgrades to the `ttasys` user.

If you try to install the software without these users and group in place, the installation program stops without making any changes to the system and displays a message telling you what you need to do. The message includes details of an install script that you can run to create the required users and group.

If you need to create the required users and group manually, the following are the requirements:

- The user names must be `ttaserv` and `ttasys`.
- The group name must be `ttaserv`.
- You can use any user identification number (UID) or group ID (GID) you want. The UID and GID can be different.
- Both users must have `ttaserv` as their primary group.
- Both users must have a valid shell, for example `/bin/sh`.
- Both users must have a *writable* home directory.
- For security, lock these accounts, for example with the `passwd -l` command.

One way to create these users is with the `useradd` and `groupadd` commands, for example:

```
# groupadd ttaserv
# useradd -g ttaserv -s /bin/sh -d /home/ttasys -m ttasys
# useradd -g ttaserv -s /bin/sh -d /home/ttaserv -m ttaserv
# passwd -l ttasys
# passwd -l ttaserv
```

To check whether the `ttasys` and `ttaserv` user accounts are correctly set up on your system, use the following commands.

```
# su ttasys -c "/usr/bin/id -a"
# su ttaserv -c "/usr/bin/id -a"
```

If your system is set up correctly, the command output should be similar to the following examples.

```
uid=1002(ttaserv) gid=1000(ttaserv) groups=1000(ttaserv)
uid=1003(ttasys) gid=1000(ttaserv) groups=1000(ttaserv)
```

1.6. Network Requirements

You must configure your network for use with SGD. The following are the main requirements:

- Hosts must have Domain Name System (DNS) entries that can be resolved by all clients.
- DNS lookups and reverse lookups for a host must always succeed.
- All client devices must use DNS.
- When you install SGD, you are asked for the DNS name to use for the SGD server. The DNS name must meet the following requirements:
  - In a network containing a firewall, use the DNS name that the SGD host is known as *inside* the firewall.
  - Always use fully-qualified DNS names for the SGD host. For example, `boston.example.com`.

The *Oracle Secure Global Desktop 4.6 Administration Guide* has detailed information about all the ports used by SGD and how to use SGD with firewalls. The following information lists the common ports used.

Client devices must be able to make Transmission Control Protocol/Internet Protocol (TCP/IP) connections to SGD on the following TCP ports:

- **80** - For Hypertext Transfer Protocol (HTTP) connections between client devices and the SGD web server. The port number can vary depending on the port selected on installation.
- **443** - For HTTP over Secure Sockets Layer (HTTPS) connections between client devices and the SGD web server.
- **3144** - For standard (unencrypted) connections between the SGD Client and the SGD server.
- **5307** - For secure connections between the SGD Client and the SGD server. Secure connections use Secure Sockets Layer (SSL).

Note

The initial connection between an SGD Client and an SGD server is *always* secure. After the user logs in to SGD, the connection is downgraded to a standard connection. When you first install SGD, TCP ports 3144 and 5307 must be open to connect to SGD. You can configure SGD to always use secure connections.

To run applications, SGD must be able to make TCP/IP connections to application servers. The types of applications determine the TCP ports that must be open, for example:

- **22** – For X and character applications using Secure Shell (SSH)
- **23** – For Windows, X, and character applications using Telnet
- **3389** – For Windows applications using Windows Terminal Services
- **6010** and above – For X applications

1.7. Clock Synchronization

In SGD, an array is a collection of SGD servers that share configuration information. As the SGD servers in an array share information about user sessions and application sessions, it is important to synchronize the clocks on the SGD hosts. Use Network Time Protocol (NTP) software or the `rdate` command to ensure the clocks on all SGD hosts are synchronized.

1.8. SGD Web Server

The SGD web server consists of an Apache web server and a Tomcat JavaServer Pages™ (JSP™) technology container preconfigured for use with SGD.

The SGD web server consists of several components. The following table lists the web server component versions for recent releases of SGD.

Component Name	SGD Version 4.62	SGD Version 4.61	SGD Version 4.60	SGD Version 4.50
`Apache HTTP Server`	2.2.21	2.2.17	2.2.16	2.2.10
`OpenSSL`	1.0.0.e	1.0.0.d	1.0.0a	0.9.8k
`mod_jk`	1.2.32	1.2.31	1.2.27	1.2.27
`Apache Jakarta Tomcat`	6.0.33	6.0.32	6.0.29	6.0.18
`Apache Axis`	1.4	1.4	1.4	1.4

The Apache web server includes all the standard Apache modules as shared objects.

The minimum Java™ Virtual Machine (JVM™) software heap size for the Tomcat JSP technology container is 256 megabytes.

1.9. Supported Authentication Mechanisms

The following are the supported mechanisms for authenticating users to SGD:

- Lightweight Directory Access Protocol (LDAP) version 3
- Microsoft Active Directory
- Network Information Service (NIS)
- Microsoft Windows Domains
- RSA SecurID
- Web server authentication (HTTP/HTTPS Basic Authentication), including public key infrastructure (PKI) client certificates

1.9.1. Supported Versions of Active Directory

Active Directory authentication and LDAP authentication are supported on the following versions of Active Directory:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

1.9.2. Supported LDAP Directories

SGD supports version 3 of the standard LDAP protocol. You can use LDAP authentication with any LDAP version 3-compliant directory server. However, SGD only supports the following directory servers:

- Oracle Directory Server Enterprise Edition version 6.3.1 and 7.0 (formerly Sun Java Directory Server Enterprise Edition)
- Microsoft Active Directory on Windows Server 2003, 2003 R2, 2008, and 2008 R2
- Novell eDirectory version 8.8

Other directory servers might work, but are not supported.

1.9.3. Supported Versions of SecurID

SGD works with versions 4, 5, 6, and 7 of RSA Authentication Manager (formerly known as ACE/Server).

SGD supports system-generated PINs and user-created PINs.

1.10. SSL Support

SGD supports TLS version 1.0 and SSL version 3.0.

SGD supports Privacy Enhanced Mail (PEM) Base 64-encoded X.509 certificates. These certificates have the following structure:

```
-----BEGIN CERTIFICATE-----
```

```
...certificate...

-----END CERTIFICATE-----
```

SGD supports the Subject Alternative Name (`subjectAltName`) extension for SSL certificates. SGD also supports the use of the `*` wildcard for the first part of the domain name, for example `*.example.com`.

SGD includes support for a number of Certificate Authorities (CAs). The `/opt/tarantella/etc/data/cacerts.txt` file contains the X.500 Distinguished Names (DNs) and MD5 signatures of all the CA certificates that SGD supports. Additional configuration is required to support SSL certificates signed by an unsupported CA. Intermediate CAs are supported, but additional configuration might be required if any of the certificates in the chain are signed by an unsupported CA.

SGD supports the use of external hardware SSL accelerators, with additional configuration.

SGD supports the following cipher suites:

- RSA_WITH_AES_256_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_DES_CBC_SHA

1.11. Printing Support

SGD supports two types of printing: PDF printing and Printer-Direct printing.

For PDF printing, SGD uses Ghostscript to convert print jobs into Portable Document Format (PDF) files. At least version 6.52 of Ghostscript must be installed on the SGD host. Your Ghostscript distribution must include the `ps2pdf` program. For best results, install the latest version of Ghostscript.

SGD supports Printer-Direct printing to PostScript, Printer Command Language (PCL), and text-only printers attached to the user's client device. The SGD `tta_print_converter` script performs any conversion needed to format print jobs correctly for the client printer. The `tta_print_converter` script uses Ghostscript to convert from Postscript to PCL. To support this conversion, Ghostscript must be installed on the SGD server. For best results, download and install the additional fonts.

Ghostscript is not included with the SGD software.

2. Client Device Requirements and Support

This section describes the supported platforms and requirements for client devices.

2.1. Supported Client Platforms

The following table lists the supported client platforms for the SGD Client. Also included are the supported browsers, and the supported desktop menu systems when the SGD Client is operating in Integrated mode.

Supported Client Platform	Supported Browsers	Integrated Mode Support
Microsoft Windows 7 (32-bit and 64-bit)	Internet Explorer 8	Microsoft Windows Start Menu

Supported Client Platform	Supported Browsers	Integrated Mode Support
	Mozilla Firefox 3	
Microsoft Windows Vista (32-bit and 64-bit)	Internet Explorer 7 Internet Explorer 8 Mozilla Firefox 3	Microsoft Windows Start Menu
Microsoft Windows XP Professional (32-bit)	Internet Explorer 7 Internet Explorer 8 Mozilla Firefox 3	Microsoft Windows Start Menu
Oracle Solaris on SPARC platforms At least Oracle Solaris 10 10/09	Mozilla Firefox 3	Java Desktop System Launch Menu
Oracle Solaris on x86 platforms At least Oracle Solaris 10 10/09	Mozilla Firefox 3	Java Desktop System Launch Menu
Oracle Solaris Trusted Extensions on SPARC platforms At least Oracle Solaris 10 10/09	Mozilla Firefox 3	Not supported
Oracle Solaris Trusted Extensions on x86 platforms At least Oracle Solaris 10 10/09	Mozilla Firefox 3	Not supported
Mac OS X 10.6	Safari 5 Safari 4 Mozilla Firefox 3	Not supported
Red Hat Enterprise Linux 5.5 Desktop (32-bit and 64-bit)	Mozilla Firefox 3	Gnome or KDE Start Menu
Ubuntu 10.04 (32-bit and 64-bit)	Mozilla Firefox 3	Gnome Start Menu

The SGD Administration Console is not supported on Safari browsers.

Beta versions or preview releases of browsers are not supported.

Browsers must have the JavaScript™ programming language enabled.

To support the following functionality, browsers must have Java™ technology enabled:

- Downloading and installing the SGD Client automatically
- Determining proxy server settings from the user's default browser

If Java technology is not available, the SGD Client can be downloaded and installed manually. Manual installation is available for all supported client platforms except Mac OS X. On Microsoft Windows platforms, you need administrator privileges to install the SGD Client.

Java™ Plugin tool version 1.6 is supported as a plug-in for Java technology.

When users start more than one user session using the same client device and browser, the user sessions join rather than the new session ending the existing session. For user sessions to join in this way, the browser must be configured to allow permanent cookies. If permanent cookies are not allowed, user sessions always end and this might cause application windows to disappear.

For best results, client devices must be configured for at least 256 colors.

The SGD Client and webtop are available in the following supported languages:

- French
- German
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

2.1.1. Virtualization Support

The supported client platforms for SGD are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

2.1.2. Retirements to Supported Client Platforms

The following table shows the SGD Client installation platforms, browsers and Java Plugin tools that have been retired.

SGD Version	Platforms No Longer Supported
4.60	Mac OS X 10.5 OpenSolaris (all versions) Red Hat Enterprise Linux Desktop 5.0 to 5.4 Solaris 10 OS up to, and including, 5/09 Ubuntu 8 Firefox 2 Internet Explorer 6 Safari 2 Safari 3 Java Plugin tool version 1.5
4.50	Fedora Linux 8 Mac OS X 10.4 Microsoft Windows 2000 Professional

SGD Version	Platforms No Longer Supported
	Solaris 8 OS Solaris 9 OS SUSE Linux Enterprise Desktop 10 Ubuntu 7.04

2.2. Supported Proxy Servers

To connect to SGD using a proxy server, the proxy server must support tunneling. You can use HTTP, Secure (SSL) or SOCKS version 5 proxy servers.

For SOCKS version 5 proxy servers, SGD supports the Basic and No Authentication Required authentication methods. No server-side configuration is required.

2.3. PDF Printing Support

To be able to use PDF printing, a PDF viewer must be installed on the client device. SGD supports the following PDF viewers by default.

Client Platform	Default PDF Viewer
Microsoft Windows platforms	Adobe Reader, at least version 4.0
Oracle Solaris on SPARC platforms	Adobe Reader (`acroread`) GNOME PDF Viewer (`gpdf`)
Oracle Solaris on x86 platforms	GNOME PDF Viewer (`gpdf`)
Linux	GNOME PDF Viewer (`gpdf`) Evince Document Viewer (`evince`) X PDF Reader (`xpdf`)
Mac OS X	Preview App (`/Applications/Preview.app`)

Note

The Adobe Reader PDF viewer must support the `-openInNewWindow` command option. The Preview App PDF viewer must support the `open -a` command option.

To be able to use a supported PDF viewer, the application must be on the user's `PATH`.

Support for alternative PDF viewers can be configured in the user's client profile.

2.4. Supported Smart Cards

SGD works with any Personal Computer/Smart Card (PC/SC)-compliant smart card and reader supported for use with Microsoft Remote Desktop services.

3. SGD Gateway Requirements and Support

This section describes the supported platforms and requirements for the SGD Gateway.

3.1. Supported Installation Platforms for the SGD Gateway

The supported installation platforms for the *SGD Gateway host* are shown in the following table.

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	At least Oracle Solaris 10 10/09
Oracle Solaris on x86 platforms	At least Oracle Solaris 10 10/09
Red Hat Enterprise Linux (32-bit and 64-bit)	5.5
Oracle Enterprise Linux (32-bit and 64-bit)	5.5

By default, the SGD Gateway is configured to support a maximum of 100 simultaneous HTTP connections and 512 simultaneous Adaptive Internet Protocol (AIP) connections. The JVM memory size is optimized for this number of connections. Appendix C of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* has details of how to tune the Gateway for the expected number of users.

3.1.1. Virtualization Support

The supported installation platforms for the SGD Gateway are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

On Oracle Solaris 10, installation in zones is *not supported*.

3.1.2. Retirements to Supported Gateway Installation Platforms

The following table shows the SGD Gateway installation platforms that have been retired.

SGD Version	Platforms No Longer Supported
4.60	OpenSolaris (all versions) Red Hat Enterprise Linux 5.0 to 5.4 Solaris 10 OS up to, and including, 5/09 SUSE Linux Enterprise Server 10
4.50	Not applicable

3.2. SGD Server Requirements for the SGD Gateway

The following requirements apply for the SGD servers used with the SGD Gateway:

- **Secure mode.** By default, the SGD Gateway uses secure connections to SGD servers. You must enable secure connections on your SGD servers. Firewall forwarding must not be enabled.
- **Integrated mode.** SGD Clients must not be configured to access the SGD servers in Integrated mode.
- **SGD version.** The SGD servers must be running at least version 4.5 of SGD. It is best to use version 4.6 of the Gateway with version 4.6 of SGD.
- **Clock synchronization.** It is important that the system clocks on the SGD servers and the SGD Gateway are in synchronization. Use Network Time Protocol (NTP) software, or the `rdate` command, to ensure that the clocks are synchronized.

3.3. Apache Web Server

The Apache web server supplied with the SGD Gateway is Apache version 2.2.17. It includes the standard Apache modules for reverse proxying and load balancing. The modules are installed as Dynamic Shared Object (DSO) modules.

3.4. Supported Cipher Suites for SSL Connections

The SGD Gateway supports the following cipher suites for SSL connections:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

4. Application Requirements and Support

This section describes the supported platforms and requirements for displaying applications through SGD.

4.1. Supported Applications

You can use SGD to access the following types of applications:

- Microsoft Windows
- X applications running on Oracle Solaris, Linux, HP-UX, and AIX application servers
- Character applications running on Oracle Solaris, Linux, HP-UX, and AIX application servers

- Applications running on IBM mainframe and AS/400 systems
- Web applications, using Hypertext Markup Language (HTML) and Java™ technology

SGD supports the following protocols:

- Microsoft Remote Desktop Protocol (RDP) at least version 5.2
- X11
- HTTP
- HTTPS
- SSH at least version 2
- Telnet VT, American National Standards Institute (ANSI)
- TN3270E
- TN5250

4.2. Supported Installation Platforms for the SGD Enhancement Module

The SGD Enhancement Module is a software component that can be installed on an application server to provide the following additional functionality when using applications displayed through SGD:

- Advanced load balancing
- Client drive mapping (UNIX® or Linux platforms only)
- Seamless windows (Windows platforms only)
- Audio (UNIX or Linux platforms only)

The following table lists the supported installation platforms for the SGD Enhancement Module.

Operating System	**Supported Versions**
Microsoft Windows (64-bit)	Windows Server 2008 R2
Microsoft Windows (32-bit and 64-bit)	Windows Server 2008 Windows Server 2003 R2 Windows Server 2003
Oracle Solaris on SPARC platforms	8, 9, 10, 10 Trusted Extensions
Oracle Solaris on x86 platforms	10, 10 Trusted Extensions
Red Hat Enterprise Linux (32-bit and 64-bit)	5
Oracle Enterprise Linux (32-bit and 64-bit)	5
SUSE Linux Enterprise Server (32-bit and 64-bit)	10, 11

On Oracle Solaris 10 Trusted Extensions platforms, only advanced load balancing is supported. Audio and CDM are *not supported*.

Application servers that are not supported platforms for the SGD Enhancement Module can be used with SGD to access a supported application type using any of the supported protocols.

4.2.1. Virtualization Support

The supported installation platforms for the SGD Enhancement Module are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

Installation in zones is supported for Oracle Solaris 10. SGD can be installed in the global zone, or in one or more non-global zones. Installation in both the global zone and a non-global zone is *not supported*.

On Oracle Solaris 10 Trusted Extensions platforms, you must install SGD in a labeled zone. Do not install SGD in the global zone.

4.2.2. Retirements to Supported Installation Platforms for the SGD Enhancement Module

The following table shows the installation platforms for the SGD Enhancement Module that have been retired.

SGD Version	Platforms No Longer Supported
4.60	OpenSolaris (all versions) Windows Vista Business Windows Vista Professional Windows XP Professional
4.50	Fedora Linux 8 Red Hat Enterprise Linux 4 SUSE Linux Enterprise Server 9 SUSE Linux Enterprise Server 10 Windows 2000 Server

Note

The SGD Enhancement Module no longer provides functionality that is supported on Windows Vista and Windows XP platforms. These platforms are still supported as an application server platform, see Section 4.3, “Microsoft Windows Terminal Services” .

4.3. Microsoft Windows Terminal Services

SGD does not include licenses for Microsoft Windows Terminal Services. If you access terminal server functionality provided by Microsoft operating system products, you need to purchase additional licenses to use such products. Consult the license agreements for the Microsoft operating system products you are using to determine which licenses you must acquire.

Note

From Microsoft Windows Server 2008 R2, Windows Terminal Services is renamed Remote Desktop Services.

SGD supports RDP connections to the following versions of Microsoft Windows:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows 7 Ultimate
- Windows 7 Professional
- Windows Vista Ultimate
- Windows Vista Business
- Windows XP Professional

On Windows 7, Windows Vista, and Windows XP platforms, only full Windows desktop sessions are supported. Running individual applications is not supported. Seamless windows are also not supported.

The features supported by SGD depend on whether you connect using RDP or Oracle VM VirtualBox RDP (VRDP), as shown in the following table.

Table 2.1. Comparison of Features Supported by SGD When Using RDP and VRDP

Feature	RDP	VRDP
Audio recording (input audio)	✗	✗
Audio redirection	✓	✓
Clipboard redirection	✓	✓
COM port mapping	✓	✗
Compression	✓	✗
Drive redirection (client drive mapping)	✓	✗
Multi-monitor	✗	✗
Network security (encryption level)	✓	✓
Session directory	✓	✗
Smart card device redirection	✓	✗
Time zone redirection	✓	✗
USB device redirection	✗	✗
Video acceleration	✗	✗
Windows printer mapping (client printing)	✓	✗

4.3.1. Audio Quality

Windows Server 2008 R2 and Windows 7 support audio bit rates of up to 44.1 kHz. By default, SGD supports bit rates of up to 22.05 kHz. To support bit rates of up to 44.1 kHz, in the Administration Console go to the Global Settings, Client Device tab and select the Windows Audio: High Quality option.

4.3.2. Color Depth

SGD supports 8-bit, 16-bit, 24-bit, and 32-bit color depths in a Windows Terminal Server session.

32-bit color is available on Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7 platforms. To display 32-bit color, the client device must be capable of displaying 32-bit color.

15-bit color depths are not supported. If this color depth is specified on the Terminal Server, SGD automatically adjusts the color depth to 8-bit.

4.3.3. Encryption Level

You can only use the Low, Client-compatible, or High encryption levels with SGD. SGD does not support the Federal Information Processing Standards (FIPS) encryption level.

4.3.4. Transport Layer Security

From Microsoft Windows Server 2003, you can use Transport Layer Security (TLS) for server authentication, and to encrypt Terminal Server communications. SGD does not support the use of TLS.

4.4. X and Character Applications

To run X and character applications, SGD must be able to connect to the application server that hosts the application. SGD supports SSH, Telnet, and rexec as connection methods. SSH is the best for security.

SGD works with SSH version 2 or later. Because of SSH version compatibility problems, use the same major version of SSH, either version 2 or version 3, on all SGD hosts and application servers.

If you are using SSH to connect to X applications, you must enable X11 forwarding. You can do this either in your SSH configuration or by configuring the application in SGD. The *Oracle Secure Global Desktop 4.6 Administration Guide* has details on using SSH with SGD.

SGD supports the X Security extension. The X Security extension only works with versions of SSH that support the `-Y` option. For OpenSSH, this is version 3.8 or later

4.4.1. Supported X Extensions

SGD includes an X server, based on X11R6.8.2.

SGD supports the following X extensions for X applications:

- BIG-REQUESTS
- BLINK
- DAMAGE
- DEC-XTRAP
- DOUBLE-BUFFER
- Extended-Visual-Information
- GLX
- MIT-SCREEN-SAVER
- MIT-SHM
- MIT-SUNDRY-NONSTANDARD
- NATIVE-WND

- RDP
- RECORD
- RENDER
- SCO-MISC
- SECURITY
- SGI-GLX
- SHAPE
- SYNC
- TOG-CUP
- X-Resource
- XC-APPGROUP
- XC-MISC
- XFIXES
- XFree86-Bigfont
- XTEST
- XTTDEV

The following X extensions are *not* supported:

- KEYBOARD
- RANDR
- XINERAMA
- XVIDEO

4.4.2. Character Applications

SGD supports VT420, Wyse 60, or SCO Console character applications

4.5. Virtual Desktop Infrastructure

In SGD version 4.60, a new type of object called a *dynamic application server* was introduced. A dynamic application server is an object that represents a virtual server broker (VSB). SGD uses the VSB to obtain a list of application servers that can run an application.

SGD includes a VDI broker that enables you to give users access to desktops provided by an Oracle Virtual Desktop Infrastructure (VDI) server.

The following versions of VDI are supported:

- Oracle VDI 3.2.2

- Sun VDI 3.1.1

See Oracle Support Knowledge Document 1373652.1 if you want to use SGD with other versions of VDI.

5. Deprecated Features

In SGD version 4.60 the Citrix Independent Computing Architecture (ICA) protocol is no longer available as a protocol for connecting to Windows applications servers. As an alternative, you can configure the Citrix ICA Client as an X application object.

The following SGD features might not be available in the next release of SGD:

- SGD load-balancing JSP (`swcd.jsp`). The SGD Gateway provides a much better solution for load-balanced deployments.
- Windows domain authentication. Use Active Directory authentication instead.
- SecurID authentication. Use the RSA Authentication Agent with third-party authentication instead.
- Integrated mode for the SGD Client.
- Running applications on local Windows client devices (known as local launch).
- The `tarantella cache` command.

Chapter 3. Known Issues, Bug Fixes, and Documentation Issues

This chapter contains information about known issues, bug fixes, and documentation issues for Oracle Secure Global Desktop (SGD).

1. Known Bugs and Issues

This section lists the known bugs and issues with SGD version 4.62.

1.1. 2205237 - Seamless Windows Display Problems When Restarting a Disconnected Session

Problem: Issues with seamless windows might be encountered when the user restarts a Windows application after closing it down. The problem is seen when the application is hosted on a Window Server 2008 R2 server.

Cause: A known problem with some versions of the SGD Enhancement Module.

Solution: Ensure that the version of the SGD Enhancement Module running on the Windows application server is the same as the SGD server version.

1.2. 6456278 - Integrated Mode Does Not Work for the Root User

Problem: On Solaris 10 OS x86 platforms, enabling Integrated mode when you are logged in as the `root` user does not add applications to the Solaris 10 Launch menu. You might also see the following warning:

```
gnome-vfs-modules-WARNING **: Error writing vfolder configuration file
"//.gnome2/vfolders/applications.vfolder-info": File not found.
```

Cause: A known issue with the Gnome Virtual File System (VFS).

Solution: No solution is currently available.

1.3. 6482912 - SGD Client Not Installed Automatically

Problem: Using Internet Explorer 7 on Microsoft Windows Vista platforms, the SGD Client cannot be downloaded and installed automatically. The SGD Client can be installed manually and can be installed automatically using another browser, such as Firefox.

Cause: Internet Explorer has a Protected Mode that prevents the SGD Client from downloading and installing automatically.

Solution: Add the SGD server to the list of Trusted Sites in Internet Explorer's Security Settings.

1.4. 6555834 – Java™ Technology is Enabled For Browser But Is Not Installed On Client Device

Problem: If Java technology is enabled in your browser settings, but a Java Plugin tool is not installed on the client device, the SGD webtop does not display. The login process halts at the splash screen.

Cause: SGD uses the browser settings to determine whether to use Java technology.

Solution: Install the Java Plugin tool and create a symbolic link from the browser plug-ins directory to the location of the Java™ Virtual Machine (JVM™) software. Refer to your browser documentation for more information.

1.5. 6598048 – French Canadian Keyboard Not Mapped Correctly for Windows Applications

Problem: When using a Canadian French (legacy) keyboard layout with Windows applications, some French characters are printed incorrectly.

Cause: A known issue with Canadian French (legacy) keyboard layouts.

Solution: No known solution. A compatible keymap file is not supplied with SGD at present.

1.6. 6665330 – Font Errors When Starting VirtualBox™ Software From a Java Desktop System Session Displayed Using MyDesktop

Problem: On Solaris 10 OS, font errors are reported and there are display problems when starting the VirtualBox software from a Java Desktop System desktop session that is displayed using MyDesktop. The problem is seen when using `Xsession.jds` as the Application Command for the MyDesktop application object.

Cause: Unavailable fonts on the SGD X server.

Solution: When starting the VirtualBox software from the Java Desktop System desktop session, use the `-fn` option to specify valid fonts. Alternatively, install the missing fonts on the SGD server. See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about using fonts with SGD.

1.7. 6801579 – Kana Mode Unavailable for Solaris OS Applications on Microsoft Windows Client Devices

Problem: On Microsoft Windows client devices with Japanese locales, Kana mode is not available for Solaris OS applications.

Cause: On Microsoft Windows client devices, the SGD Client uses ASCII for Kana mode. Solaris OS applications use Unicode for Kana mode.

Solution: On the Microsoft Windows client device, add a new system variable `TARANTELLA_KEYBOARD_KANA_SOLARIS`. Set the value of this system variable to `1`.

1.8. 6809365 – Application Start Failures and Quotation Marks in the User's DN

Problem: When using LDAP to authenticate users, Windows applications can fail to start if the distinguished name (DN) of the user contains more than one single straight quotation mark (`'`).

Cause: A known issue.

Solution: The workaround is to edit the `wcpwts.exp` login script. This script is in the `/opt/tarantella/var/serverresources/expect` directory on the SGD server.

Locate the following entry in the `wcpwts.exp` script:

```
regsub {'} $value {'"'"'} value
```

Edit the entry to read as follows:

```
regsub -all {'} $value {'"'"'} value
```

1.9. 6831480 – Backup Primaries List Command Returns an Error

Problem: Using the `tarantella array list_backup_primaries` command on an SGD server that has been stopped and then detached from an array returns a “Failed to connect” error.

Cause: A known issue.

Solution: Restart the detached SGD server before using the `tarantella array list_backup_primaries` command.

1.10. 6863153 – HyperTerminal Application Hangs in a Relocated Windows Desktop Session

Problem: Users running the HyperTerminal application in a Windows desktop session experience problems when they try to resume the desktop session from another client device. The HyperTerminal application is unresponsive and cannot be closed down.

Cause: A known issue with HyperTerminal when resuming Windows desktop sessions from another client device (also called “session grabbing”).

Solution: Close down the HyperTerminal application before you resume the Windows desktop session from another client device.

1.11. 6921995 – Load-Balancing JSP Does Not Work When Java Technology is Not Available

Problem: The load-balancing JavaServer Page (JSP) used by SGD for load balancing of user sessions does not work. A Java warning message might be shown.

Cause: To use the load-balancing JSP, Java technology must be enabled on the client device.

Solution: Do one of the following:

- Enable Java technology in the browser on the client device.
- Use the SGD Gateway to load balance user sessions. This is the preferred solution, as the load-balancing JSP might not be available in future releases. See the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* for details of how to install and configure the SGD Gateway.

1.12. 6937146 – Audio Unavailable for X Applications Hosted on 64-Bit Linux Application Servers

Problem: Audio might not play in X applications that are hosted on 64-bit Linux application servers. The issue is seen for X applications that are hard-coded to use the `/dev/dsp` or `/dev/audio` device, and the Audio Redirection Library (`--unixaudiopreload`) attribute is enabled.

Cause: A known issue. A 64-bit SGD Audio Redirection Library is not included in the SGD Enhancement Module.

Solution: No known solution at present.

1.13. 6942981 – Application Startup is Slow on Solaris 10 OS Trusted Extensions

Problem: On Solaris 10 OS Trusted Extensions platforms, startup times for Windows applications and X applications might be longer than expected.

Cause: By default, the X Protocol Engine attempts to connect to X display port 10. This port is unavailable when using Solaris 10 OS Trusted Extensions. After a period of time, the X Protocol Engine connects on another X display port and the application starts successfully.

Solution: Do either of the following:

- Change the default minimum display port used by the SGD server.

  Configure the following setting in the `xpe.properties` file in the `/opt/tarantella/var/serverconfig/local` directory on the SGD server:

  ```
  tarantella.config.xpeconfig.defaultmindisplay=11
  ```

  Restart the SGD server after making this change.

- Exclude the unavailable port from use by the X Protocol Engine.

  In the Administration Console, go to the Protocol Engines, X tab for each SGD server in the array and type `-xport` *`portnum`* in the Command-Line Arguments field, where *`portnum`* is the TCP port number to exclude.

  Alternatively, use the following command:

  ```
  $ tarantella config edit --xpe-args "-xport portnum"
  ```

  For example, to exclude X display port 10 from use by the X Protocol Engine:

  ```
  $ tarantella config edit --xpe-args "-xport 6010"
  ```

  The changes made take effect for new X Protocol Engines only. Existing X Protocol Engines are not affected.

1.14. 6957820 – SGD Client Hangs When Using Smart Card Authentication for Windows Applications

Problem: When using a smart card to log in to a Windows application session from a Ubuntu 10.04 Linux client device, the SGD Client hangs after the user exits the authenticated application session. The user might not be able to start any further applications or log out from SGD.

Cause: A known issue with version 1.5.3 of PCSC-Lite on Ubuntu client platforms.

Solution: Update to the latest version of PCSC-Lite on the client device.

1.15. 6961236 – Error Messages in Tomcat Log

Problem: Error messages about ThreadLocal memory leaks are written to the Tomcat JSP container log file at `/opt/tarantella/webserver/tomcat/`*`tomcat-version`*`/logs/catalina.out`. Operation of SGD is not affected.

Cause: A known issue with the memory leak detection feature of Tomcat.

Solution: No known solution. The issue will be fixed in future releases of Tomcat.

1.16. 6962970 – Windows Client Device Uses Multiple CALs

Problem: A Windows client device is allocated multiple client access licences (CALs). A CAL is incorrectly allocated each time a Windows application is started.

Cause: A known issue if the `HKEY_LOCAL_MACHINE\Software\Microsoft\MSLicensing` key or any of its subkeys are missing from the Windows registry on a client device. This issue affects Microsoft Windows Vista and Microsoft Windows 7 platforms.

Solution: Recreate the missing keys, by starting the Remote Desktop Connection with administrator privileges. See Microsoft Knowledge Base article 187614 for more details.

1.17. 6963320 – Cannot Connect to SGD Using Version 4.5 of the SGD Gateway, or Using an Upgraded Version 4.6 Gateway

Problem: After 90 days, users cannot connect to SGD using a version 4.5 Gateway. After upgrading a Gateway to version 4.6, users cannot connect to SGD.

Cause: Version 4.5 of the SGD Gateway uses self-signed certificates that are valid for only 90 days. This affects the default self-signed SSL certificate used for client connections to the Gateway, as well as the Gateway certificate and the certificate used for the Reflection service.

After upgrading a Gateway to version 4.6, users cannot connect to SGD because the Gateway self-signed certificates have been replaced.

Solution: If you are using a version 4.5 Gateway, upgrade to version 4.6.

If you have upgraded a Gateway to version 4.6, you need to perform the standard configuration steps for authorizing a Gateway to SGD, as described in “How to Install SGD Gateway Certificates on the SGD Array” on page 16 of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide*.

In version 4.6, the Gateway certificate and the certificate for the Reflection service are valid for 3600 days. The default self-signed SSL certificate used for client connections to the Gateway is valid for 365 days. If you have installed your own SSL certificate for client SSL connections, this certificate is preserved when you upgrade.

1.18. 6969404 – PDF Printing Issue on Solaris 10 OS Platforms

Problem: Portable Document Format (PDF) printing might not work on Solaris 10 10/09 platforms. The PDF file displays PostScript™ error messages.

Cause: A known issue with some versions of Ghostscript. SGD uses Ghostscript to convert print jobs into PDF files.

Solution: Install the latest version of Ghostscript on the SGD server. Ensure that the symbolic link `/opt/tarantella/var/info/gsbindir` points to the directory where the new Ghostscript binaries are installed.

This fix has been verified using version 8.71 of Ghostscript.

1.19. 6970615 – SecurID Authentication Fails for X Applications

Problem: SecurID authentication for X applications fails when using the RSA Authentication Agent for PAM. The issue is seen with X applications that are configured to use telnet as the Connection Method.

Cause: A known issue when using the RSA Authentication Agent for PAM.

Solution: Configure the X application object to use SSH as the Connection Method.

1.20. 6974464 – Kiosk Mode Display Issue on Ubuntu Clients

Problem: On Ubuntu client platforms, applications displayed in kiosk mode are obscured by the Ubuntu desktop toolbars. The issue is seen when the Compiz window manager is used and visual effects are enabled for the Ubuntu desktop.

Cause: The Compiz window manager does not provide legacy full screen support by default.

Solution: Do either of the following:

- Turn off visual effects for the Ubuntu desktop.
- Install the Compiz Config Settings Manager and enable the Legacy Fullscreen Support option in the Workarounds plugin.

Changes made only take effect for new application sessions.

1.21. 6979110 – Localized Documentation Not Available

Problem: Localized HTML documentation is not available. English documentation is displayed instead.

Cause: A known issue.

Solution: PDF versions of the localized documentation are available from the SGD web server Welcome Page.

1.22. 7004887 – Print to File Fails for Windows Client Devices

Problem: When users select the Print to File menu option in a Windows application displayed through SGD, the print job remains on hold in the print queue on the client device. The issue is seen on Windows Vista and Windows 7 client devices.

Cause: A known issue with some versions of Windows.

Solution: A workaround for Windows Vista is described in Microsoft Knowledge Base article 2022748.

1.23. 7014475 – LDAP Login Filters Are Not Preserved on Upgrade

Problem: LDAP login filters are not preserved when you upgrade to version 4.6 of SGD.

Cause: Because of LDAP enhancements introduced in SGD 4.6, any customizations you have made to the LDAP login filters are not preserved on upgrade. See Section 1.3, “Active Directory and LDAP Enhancements” for more details of the enhancements.

Solution: Reconfigure your LDAP login filters after upgrading. See the “Filtering LDAP or Active Directory Logins” section in Chapter 2 of the *Oracle Secure Global Desktop 4.6 Administration Guide* for details of how to configure LDAP login filters.

1.24. 7020250 – Audio Module Install Fails on 64-Bit SUSE Linux Platforms

Problem: When installing the SGD Enhancement Module on 64-bit SUSE Linux platforms, installation of the UNIX audio module fails. The issue is seen when installing on SUSE Linux Enterprise Server 11.

Cause: A known issue on 64-bit SUSE Linux platforms.

Solution: The workaround is to edit the following files in the `/opt/tta_tem/audio/src/sgdadem` directory:

- In the `Makefile` file, change all instances of `CFLAGS` to `EXTRA_CFLAGS`.

- In the `sgdadem.h` file, replace the following line:

```
#include <linux/ioctl32.h>
```

Add the following lines:

```
#include <linux/version.h>
#if LINUX_VERSION_CODE < KERNEL_VERSION(2,6,22)
#include <linux/ioctl32.h>
#endif
```

After making the changes to the `sgdadem.h` file, run the following commands to install and start the audio module.

```
# cd /opt/tta_tem/audio/src/sgdadem
# make
# make install
# /opt/tta_tem/bin/tem startaudio
```

1.25. 7022104 – Automatic Configuration of Secure Connections Fails on an Upgraded Server

Problem: Using automatic configuration to reconfigure secure connections fails on an SGD server that has been upgraded to version 4.6. The issue is seen on upgraded servers that have previously been configured for secure connections automatically, using the `tarantella config enable` command.

Errors are reported when you use the `tarantella security disable` command to restore original security settings.

Cause: A known issue when using `tarantella security disable` on an upgraded server.

Solution: Run `tarantella security disable` on the server *before* you upgrade. Secure connections can then be configured automatically on the upgraded server, by running `tarantella security enable`.

1.26. 12309146 – Administrators Unable to Search Parent OUs in Active Directory

Problem: LDAP searches into parent organizational units (OUs) in Active Directory do not return any results. The issue is seen in the Administration Console when assigning applications to LDAP users using Directory Services Integration (DSI). LDAP searches into child OUs are unaffected.

Cause: A known issue with the LDAP search filter generated by the Administration Console.

Solution: The workaround is to modify the LDAP search filter.

In the Administration Console, go to the Assigned User Profiles tab for the application object.

In the Advanced Search section, append an `(objectclass=*)` entry to the LDAP search filter. For example:

```
ldap:///OU=Users,OU=Marketing,DC=example,DC=com,DC=uk??sub?(objectclass=*)
```

1.27. 12309185 – Cached LDAP Passwords Fail After an Upgrade

Problem: Cached passwords for some LDAP users may no longer work following an upgrade from version 4.50.

Cause: A known issue. The naming format for storing LDAP password cache entries has changed since SGD 4.50.

Solution: Contact Oracle Support or see `https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1316990.1` for details of how to migrate password cache entries.

1.28. 12309385 – Gateway Protocol Translation Fails from HTTPS to HTTP

Problem: Users are unable to start applications, or to access the Administration Console. The issue is seen when the SGD Gateway is configured to use unencrypted HTTP connections between the Gateway and the SGD servers in the array.

Cause: A known issue when connections between the Gateway and the SGD servers in the array are not secure. By default, these connections are secure.

Solution: The workaround is to edit the Apache reverse proxy configuration file at `/opt/SUNWsgdg/httpd/apache-version/conf/extra/gateway/httpd-gateway.conf`.

Comment out the following entry:

```
ProxyPassReverse / https://gateway.example.com:443/
```

Add the following entries:

```
ProxyPassReverse / http://gateway.example.com/
ProxyPassReverse / http://gateway.example.com:80/
```

where *gateway.example.com* is the name of the SGD Gateway.

1.29. 12309559 – Java Detection Fails When Using Internet Explorer 9

Problem: The Java Plugin tool is installed on the client device and Java technology is enabled in your browser settings, but SGD reports that Java is not enabled or installed for the browser. The issue is seen when logging in to SGD using Internet Explorer 9 on Windows client platforms.

Cause: A known issue when using this version of Internet Explorer.

Solution: Use one of the following workarounds.

- Before logging in to SGD, enable compatibility view for Internet Explorer. See Microsoft Knowledge Base article 956197 for details of how to do this.
- When the Java detection error message is displayed, click the Back button on the browser. To use this workaround, the SGD Client icon must be present in the task bar and should indicate that a connection has been established.

1.30. 13117149 – Accented Characters in Active Directory User Names

Problem: Active Directory authentication fails for user names that contain accented characters, such as the German umlaut character (ü).

The following error is shown in the log output when using the `server/login/info` log filter:

```
javax.security.auth.login.LoginException: Integrity check on decrypted field failed (31)
```

Cause: Active Directory authentication uses the Kerberos authentication protocol. This is a known issue when Kerberos authentication is configured to use DES encryption.

Solution: The workaround is to disable the use of DES encryption in the `krb5.conf` Kerberos configuration file on the SGD server.

Include the following lines in the `[libdefaults]` section of the `krb5.conf` file.

```
  [libdefaults]
```

```
   default_tgs_enctypes =  rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
   default_tkt_enctypes =  rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
```

1.31. 13242998 – Configuring Ciphers for the SGD Gateway

Problem: Secure connections to the Gateway using SSL do not alway use high grade ciphers.

Cause: By default, the Gateway supports a wide range of cipher suites, including some low and medium grade ciphers.

See Section 3.4, “Supported Cipher Suites for SSL Connections” for a list of supported cipher suites for SSL connections.

Solution: Configure the Gateway to use a specific set of ciphers, as follows:

- Stop the Gateway.

```
# /opt/SUNWsgdg/bin/gateway stop
```

- In the `/opt/SUNWsgdg/etc` directory create a file called `ciphersuites.xml` that contains a list of the required ciphers. For example:

```
<ciphersuites>
 <cipher>SSL_RSA_WITH_RC4_128_MD5</cipher>
 <cipher>SSL_RSA_WITH_RC4_128_SHA</cipher>
 <cipher>TLS_RSA_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_RSA_WITH_AES_256_CBC_SHA</cipher>
 <cipher>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</cipher>
 <cipher>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_DHE_DSS_WITH_AES_256_CBC_SHA</cipher>
 <cipher>SSL_RSA_WITH_3DES_EDE_CBC_SHA</cipher>
 <cipher>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</cipher>
 <cipher>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</cipher>
</ciphersuites>
```

- Add the following entries to the `/opt/SUNWsgdg/etc/gateway.xml` file, so that it includes `ciphersuites.xml`.

```
<service id="sgd-ssl-service" class="SSL">
                ...
  <keystore file="/opt/SUNWsgdg/proxy/etc/keystore.client"
   password="/opt/SUNWsgdg/etc/password"/>
   <xi:include href="ciphersuites.xml" parse="xml"/>
</service>
                ...
<service id="http-ssl-service" class="SSL">
                ...
  <keystore file="/opt/SUNWsgdg/proxy/etc/keystore.client"
   password="/opt/SUNWsgdg/etc/password"/>
  <xi:include href="ciphersuites.xml" parse="xml"/>
</service>
```

- Restart the Gateway.

```
# /opt/SUNWsgdg/bin/gateway start
```

1.32. Sun Type 7 Japanese Keyboard Issues

Problem: Users with Sun Type 7 Japanese keyboards cannot input characters correctly using SGD.

Cause: Missing Solaris OS keytable on the client device.

Solution: Install the appropriate patch to install the keytable on the client device.

Platform	Patch
Solaris 10 OS on SPARC platforms	121868
Solaris 10 OS on x86 platforms	121869

1.33. Start Menu Items Not Sorted Alphabetically

Problem: When using the SGD Client in Integrated mode on Microsoft Windows client devices, users might notice that the Start menu entries are not sorted alphabetically.

Cause: This is caused by a Windows feature that adds new items to end of a menu, rather than preserving the alphabetical sorting.

Solution: See Microsoft Knowledge Base article 177482 for details.

1.34. Microsoft Windows Server 2003 Applications Limited to 8-Bit Color Depth for Large Screen Resolutions

Problem: For Microsoft Windows Server 2003 applications, the display color depth on the client device is limited to 8-bit for large screen resolutions. The issue is seen when screen resolutions are higher than 1600 x 1200 pixels.

Cause: A known issue with Windows Server 2003 terminal services sessions.

Solution: See Microsoft Hotfix 942610 for details of how to increase the color depth to 16-bit.

2. Bug Fixes in Version 4.62

The following table lists the significant bugs that are fixed in the 4.62 release.

Table 3.1. Bugs Fixed in the 4.62 Release

Reference	Description
12280889	User groups with apostrophe character are not created correctly.
12301550	Character order is sporadically mixed up for Windows applications.
12302888	Maximum CPU load on Gateway when using client certificates.
12303230	Connecting to Gateway fails when using a non-Java client.
12306818	Errors when using `tarantella restart` on upgraded server.
12308408	Connection failures when using `.pac` file with Gateway.
12320939	Version 4.50 Gateway stops accepting connections.
12334799	Connections from SGD 4.50 to VDI 3.2.1 fail when using VRDP.
12539456	Typing µ (shift + *) on French keyboard does not work.
12542674	Users unable to log in to SGD Gateway version 4.50.907.
12564490	No objects on Administrator webtop after upgrading to SGD 4.61.
12591841	Non-existent emulator sessions reported by `tarantella emulatorsession list`.
12800592	SGD audio module logs many debug messages to `dmesg`.
12835503	Service object URLs do not support Chinese characters.
12943912	Warm restart of SGD server does not preserve sessions.
13025314	Unable to access SGD Administration Console using the Gateway.

Reference	Description
13035086	Symbolic link errors when upgrading SGD.
13038431	Tar errors when upgrading SGD.
13071679	Gateway failures when under heavy user load.
13096271	Active Directory passwords are visible when `server/login/moreinfo` log filter is enabled.
13105995	Users unable to update Active Directory passwords.
13261681	Changing AD password sends user back to login page.
13422998	Configuring high grade ciphers for the SGD Gateway.

3. Bug Fixes in Version 4.61

The following table lists the significant bugs that are fixed in the 4.61 release.

Table 3.2. Bugs Fixed in the 4.61 Release

Reference	Description
220322	Application launch periodically fails with `"connect /tmp/.X11-unix/X10: No such file or ...".`
2201515	Using `needClientAuth` on the SGD Gateway causes the CPU load to go to 100%.
2202871	Since upgrade to 4.5, print jobs intermittently stay in print queue even after fix.
2202933	Application servers are lost on an upgrade from SGD 4.50.933 to SGD 4.60.911.
2203217	Support for SGD Enhancement Module on 64-bit Red Hat Linux.
2203218	Unable to toggle Caps Lock off on Linux and Mac client after enabling.
2203220	Passwords appear in clear text in log files and launch progress box after repeated failed attempts.
2203580	Cannot launch VDI desktops hosted on a Microsoft Remote Desktop provider.
2205237	After reconnecting to disconnected session, moving seamless windows application retains background (Windows Server 2008 R2).
2205239	Drive mapping (CDM) does not work in SGD 4.6 with Windows XP application server.
2205240	Unable to install and run the SGD Client on Toshiba laptop with OpenSolaris.
2205241	Hierarchical webtop fails to display any items in 4.60.911.
2205471	User session grabbing and joining causes memory leaks.
2205545	Firefox states that Gateway uses AES-128, but SGD uses AES-256.
2206552	SGD installation fails with a “Permission Denied” error from an operation on the Tomcat log file.
2206775	SGD VDI Broker does not handle multiple companies.
2207516	`ContinuationLaunch` instances are not being removed correctly from `EmulatorSessionModel.`
6987909	`tarantella object list_contents` does not list the contents of domain component (`dc=`) objects.
6989531	Server-side event notification broken.
7000468	`ArrayIndexOutOfBoundsException` on 4.50 to 4.60 upgrade.
7000574	Multiple free-text boxes on a chooser page causes all but the first to be ignored.

Reference	Description
7001553	Array members report not accepting connections after upgrade to 4.60.
7002566	Exception on upgrade to 4.60 on Solaris SPARC.
7003689	Update third party components for SGD web server.
7004887	Printing to a “Print to File” printer fails through SGD on Windows 7.
7005084	Application resume fails from another array member when using third-party authentication.
7008234	Upgrading the SGD Gateway from 4.5 to 4.6 causes a complete wipeout of configuration.
7010459	RDP printers not mapped in 4.6 for SecurID SGD users.
7010965	Need to move EOSL info from SGD Release Notes.
7011883	Use Tomcat `stop -force` option to work around Tomcat shutdown issues.
7012779	Copyright notices need updating.
7014475	Upgrade to 4.60 does not retain the customized LDAP user search attributes.
7014595	Update copyright messages to include 2011.
7014596	Review contents of `cacerts.txt` file.
7014622	Open Source and 3rd Party Matrix Approval.
7014625	Export approval for SGD.
7014863	TEM fails to install on 32-bit platform due to 64-bit library dependencies.
7015217	TEM and SGD Client InstallShield product codes need updating to support upgrades.
7016383	Launches to VDA fail if server pool uses NAT.
7017535	Administration Console reports incorrect version number.
7017907	`NullPointerException` messages in the SGD server log when session is grabbed.
7019010	OpenSSL License in `ThirdPartyReadMe.txt`.
7020361	Doc build requires minor fixes for 4.61 release.
7022929	Multiple JNDI listeners are registered for a user session.
70252161	Using `printinstall.en.sh` on Solaris returns syntax errors.
7025500	Cached LDAP passwords are lost on upgrade.
7027639	`ADLoginAuthority` bean properties not present after upgrade.
7029828	Global properties not present after upgrade.
12309461	Property incompatibilities following an upgrade.
12309968	PDF print jobs are accepted but not printed on Mac OS X clients.
12312718	Exceptions when running the `tarantella emulatorsession` command.
12351315	`--person` option does not work for `tarantella emulatorsession list` command.

4. Bug Fixes in Version 4.60

The following table lists the significant bugs that are fixed in the 4.60 release.

Table 3.3. Bugs Fixed in the 4.60 Release

Reference	Description
6499708	Active Directory user names that contain accented characters cannot login.

Reference	Description
6548584	Input method status windows are empty and break CWM applications.
6557852	SGD should detect time drift amongst array members and notify.
6577023	Unavailable KDCs cause repeated time delays for Active Directory logins.
6606611	Attempting to detach itself (secondary) from an array fails.
6611453	`tcc.exe` needs to detect non-supported options and display usage message.
6612885	German Excel shortcut (CTRL + +) does not work.
6618608	Webtop generation using LDAP groups can cause delays on login.
6620281	Errors launching and printing when using third-party profile in an array.
6634243	Vista desktop sessions limited to 16-bit, RDC 6 client supports 32-bit.
6650334	Difficulties in mirroring LDAP in local repository, based on groups, with LDAP profiles on OU.
6654307	Make Active Directory authentication site aware.
6657964	Request that directory indices be disabled in default Apache and Tomcat configuration, if unnecessary.
6679914	Java technology application displays scroll bars on dialog and panels when run in CWM mode.
6690758	Ctrl-Alt-End (Del) does not work for Mac users running Terminal services session on VirtualBox or VMware using SGD.
6693475	IME window left behind when moving X-applications.
6704363	Next button not visible by default in Internet Explorer browsers on “Change SGD Authentication Pop-up Window”.
6706042	Wrong default keymap setting for user profiles and login profiles.
6710090	Solaris OS keyboards and applications, not all compose key combinations work and depend on the locale.
6712822	Edit icon page, click on OK button does not close the window.
6713910	aacute, oacute characters missing from `xfrenchcanadian.txt`.
6715970	Surname field for user objects should have star mark indicating it as mandatory field.
6716041	Object could not be created error, when creating object after a make primary operation.
6720214	Number sign key is not generated in Russian keyboard layout.
6721595	Unable to edit files using `gedit` or `kedit` using Linux client in certain scenarios.
6722394	Input locale sh, which I think stands for Serbo-Croat, should map to `xcroatian.txt`.
6722403	Uring only works for X applications (Croatia).
6722430	Ã produces Ãn with `ttatsc` and `xswedish.txt`.
6723927	Tabbing does not work properly in UNIX SGD Client spoof dialog.
6723997	LDAP connection error message needs cleaning up.
6724408	Some strings truncated in non-English TCC dialogs.
6724412	Untranslated “Session Transferred” page title.
6726411	`ttaxpe` should ignore `xmodmap` pointer device mappings.
6731581	Need to distinguish between Return and Keypad Enter.

Reference	Description
6732667	Pasting data into CDE applications does not work.
6734004	Users with Portuguese characters in Active Directory common name (CN) lose sessions periodically 4.40.917.
6755548	Add option to resume printer state in MyDesktop.
6763595	Windows applications do not launch after changing global printer settings.
6765576	Do not need to secure soap for standard server-side listener events.
6794245	MouseMove event does not work after upgrading from 4.2 to 4.4.
6794389	Validation error message pops up when disabling the application's copy and paste security level.
6796420	Session ID cookies not marked as secure.
6796460	Disable autocomplete on login page to prevent browser caching user name and password.
6797395	`prtinstall.en.us` failed to detect SGD installation.
6798637	`ttatsc` on UNIX client fails to get a licence from 2008 servers, but still connects.
6801579	SGD 4.5 Windows Client cannot enable Kana mode for Solaris OS applications.
6802223	Message box for the SGD Client Helper does not have Sun branding or l10n.
6802825	`tarantella uninstall` should try to handle array clean up.
6805104	UNIX application audio is not routed to Vista client properly across subnets.
6805302	Unable to display all area when CWM session transferred to large resolution window.
6807223	SHIFT + DEL does not work in Terminal Services session in SGD 4.41.907.
6807557	Add support for Latin Extended Additional (UK and Ireland) 0x1E00 to 0x1EFF.
6808012	Support for support serial pass-through for UNIX application servers.
6810687	LDAP Users with long paths cannot save passwords in the password cache.
6811718	NumLock needs disabling before CTRL+F keys work.
6814983	CAPS LOCK is not working with `xgreek` keymap.
6817237	Kiosk mode only displays on one screen when used with `Xinerama`.
6818244	`InterruptedNamingException` reported by `tarantella config edit` command on secondary when the primary server is unavailable.
6822670	`tarantella start startcdm` not working on SuSE 11 (32-bit).
6822705	Printer install script fails to create `tta_printer` on SuSE 11.
6825514	`localarraydata` file not created on primary if `tarantella array join` command is run on the secondary.
6829009	Secondary windows of seamless application are drawn in background, but work fine in independent window mode.
6831498	Application settings for printing settings are not absolute.
6832477	`tarantella start/stop --array` has not been fully removed.
6834433	Input filter missing from Tomcat configuration.
6836060	Printing fails on Red Hat 5.2 if SELinux is set to enforcing.
6837245	New application sessions for all users on all array members fail to start. Existing sessions work.

Reference	Description
6838741	Copy and paste restrictions can be circumvented by cutting content rather than copying.
6839019	Hierarchical webtop is broken.
6839805	Request log messages can be prepended with host name and SSGD string.
6840581	Shortcut key combinations do not work in Emacs.
6842311	Applications run on SGD host leave temporary files.
6842532	Mac OS X 10.5.7 update prevents full screen display in Kiosk mode.
6846001	Need a way to pass an environment variable of our choosing from Sun Ray DTU to Terminal Services session through SGD.
6846596	Pasting into OpenWindows Solaris 8 OS applications does not work.
6846808	`krb5.conf` file is not preserved on upgrade.
6847515	SGD Client spins if it receives an invalid audio or serial I/O packet.
6848440	Default “My Desktop” application no longer exits when you log out.
6849891	After upgrade from 4.40.917 to 4.50.907 `tarantella start` fails.
6852198	Performance issue with CAD application.
6852617	Unable to use the Gateway with an upgraded SGD installation.
6856527	Use `XFIXES` to obtain clipboard changes.
6856981	Intermittently a wrong default printer is selected on Terminal Services sessions.
6861095	After webtop logout, the login button on the “Logged Out” page is not always a clickable link.
6861419	SGD installs startup scripts in both `rc2.d` and `rc3.d` on Solaris OS.
6862242	Alt + ‘does not toggle the IME when used in SGD.
6862717	Caps Lock state appears to stick on Windows client (repeat key problem).
6863152	Windows session crashes when the HyperTerminal application is started after a session grab.
6867328	Connection error message shown in “Detailed Diagnostics” under “Info” link of webtop.
6867790	UK keyboard map has incorrect definition for “3” key, cannot be typed within VirtualBox or VMWare console.
6869188	When only third-party authentication is enabled, you cannot enter LDAP searches for webtop generation.
6870510	SGD Administration Console’s search function does not find empty LDAP groups.
6870877	Refresh of browser at the “OK to close this window” crashes MyDesktop.
6871452	Setting `server.bindaddresses.external` needs * and does not appear to work with `!127.0.01`.
6872934	Provide support for clients that do not have Java technology.
6873367	“Object could not be created” error was seen while creating a new object in search option window.
6874184	Active Directory authentication with user name that contains umlauts fails.
6874822	Application launches fail with “Maximum number of sessions has been reached”.
6875850	“Passwords do not match” error message is corrupted in Japanese locale in change password form.

Reference	Description
6885772	Start script should detect if SGD is already running.
6886487	Option to prompt user to allow downgraded connection when SSH forwarding is not configured.
6888273	After a crash, replacement SGD Client is unable to print.
6889378	RDP session does not terminate with Enhancement Module and AFS/Kerberos software both installed.
6890490	Seamless windows applications fail when running with KDE on the client.
6893767	Leave sound at the remote host.
6893822	UNIX audio is broken.
6894284	Unable to type capital umlauts with Swiss keyboard. Key combination displays wrong character.
6896383	Caps Lock on French keyboard gives capitalized accented characters when numbers are expected.
6896391	Organizational Unit is not overriding the serial port settings of Global Settings.
6898039	Audio fails on Sun Ray when logged into webtop on Solaris Trusted Extensions.
6898102	Password cache issue seen with JDK 6 update 16.
6900586	Webtop takes a long time to display (up to 20 minutes) ,lots of errors in web server.
6902507	Need to ensure only one PID is tracked in various SGD PID files.
6902534	Update upgrade installation to handle changes to attributes.
6903480	Overhaul German keymap file.
6903481	Overhaul Czech AZERTY keymap file.
6903482	Overhaul Belgian keymap files.
6905248	`/opt/tarantella/bin/lp` command fails if the file name has spaces in it.
6905397	Some password related messages are not localized in Japanese locale.
6907461	Old settings are not preserved during Enhancement Module upgrade.
6908714	Get Service Tag identifier for SGD.
6909715	Clipboard security level cannot be saved by pressing bottom “Save” button (top one works).
6910136	PDF Printing does not work from Windows 7 application.
6912997	The Backspace/Delete key appears to behave like the End key on the Apple Mac in SGD 4.50.933.
6913651	Leaving residual image while resizing drawing using Autocad on Windows Server.
6914169	Upgrade does not recognize “`lib`” as one of the expected contents of `/opt/tarantella`.
6914391	Two or more apostrophes in a user’s distinguished name (DN) causes an application launch failure.
6914465	Upgrades fail if `httpd.conf` contains “`Listen 127.0.0.1:80`”.
6914478	If a security enabled server is upgraded, HTTP to HTTPS forwarding no longer takes place.
6916164	`NullPointerException` when creating an object when the main window is on another page.

Reference	Description
6916329	Installation and arrays need to work better with DHCP.
6917315	Attempting to View Details on a non-existent session exits Administration Console.
6917355	Intra-array security setting should be visible with `tarantella config list`.
6917710	`tarantella security disable` may fail if a server has been upgraded since `tarantella security enable` was run.
6919207	Failed to launch a session with SGD if the password contains the Backslash character at the beginning.
6919683	Update Expect scripts following removal of Citrix support.
6920543	X Protocol Engine crashes on exit.
6921236	Input methods are being deliberately disabled from the expect scripts for no good reason.
6924262	X launches fail with `ttatdmcl` error if X11 forwarding is not enabled. A better error would help.
6924650	SGD Client on 64-bit Windows stores client license separately from MSTSC license.
6925036	When switching between non-seamless and seamless window you cannot enter keyboard input.
6925509	Applications created from the command line cannot be added to a group.
6925914	Disable `SIGUSR2` handling.
6927936	Shift + F11 and Shift + F12 on a Sun keyboard cannot be mapped in SGD.
6927946	SGD Client reports incorrect launch error.
6929786	`tarantella array list_backup_primaries` is not displaying all the secondary servers from the list.
6929850	A comma in the common name causes an exception when loading LDAP assignments.
6935362	Installation fails if `ttasys` and `ttaserv` users do not have a `bash` or `sh` shell.
6935579	Backup primaries list is not updated when using the Administration Console.
6937164	Support for SGD Enhancement Module on 64-bit RedHat Linux.
6938967	`ttakpasswd` tries to make its stack executable.
6942312	Audio fails with Windows Server 2008R2 as application server and SGD 4.50.907.
6942473	Password update error messages are not consistently reported to the user.
6944181	Upgrading from 4.40.917 to 4.50.933 fails if the server has been used with firewall traversal.
6944912	Smart card connections to Windows XP or 2003 fail with "`smart card service is down`".
6948342	Secure Global Desktop Servers tab, typographical error in help text.
6950215	Need to type two backquote characters to get one.
6952467	Administration Console fails to list user and application sessions if internal and external DNS names differ.
6952950	"`makenumeric command not found`" seen during installation.
6953935	Copy and paste from client to server fails resulting in a freeze of the application window.
6954181	Server.no license expired when using Active Directory.
6955041	Non-politically correct error message.

Reference	Description
6955431	`tarantella status command` returns with no output if the array secondary is offline.
6955928	CDM still works even though it is disabled in SGD Client profile.xml.
6955975	Expired passwords not handled correctly.
6956026	Failover logging produces output even when failover is not active.
6956253	Session grab makes the first client's browser crash.
6956288	The "server restarted" web page is broken.
6956839	SGD session ends when passed to server if Windows session is disconnected (Session Directory).
6957667	Copy and paste does not work from remote to local X applications.
6957720	Problems editing the password cache with `--ldap`.
6957736	Setting `_dns` for a password cache entry still causes the application authentication dialog to display.
6958248	Proper error is not displayed when application server is filtered in Administration Console.
6958297	Support for Arabic keyboard and keymap.
6958522	Problems restarting SGD web server with `--servlet` option.
6958567	User-generated SecurID PINs are not accepted using Authentication Manager 7.1.
6958992	Webtop does not stay open while copying file to the client when session idle timeout is set.
6959071	Sort out switching to Swiss German locale from Ubuntu client.
6961027	Billing query fails.
6961272	`tarantella array join` fails on Solaris OS.
6961632	Application links on the Webtop are not highlighted properly in Internet Explorer 7.
6961720	Default Gnome terminal has wrong setting.
6961969	Application server password seen in plaintext in the "Connection Progress" dialog.
6962405	My cursor is yellow and it should not be.
6962712	`/tmp/SGDWebServiceCalls.log` should probably be somewhere else.
6963320	How do you import a new server certificate into the Gateway keystore.
6963462	Application launch tab does not work in SGD 4.60 localized Administration Console.
6964177	XFSv2 cross-frame scripting vulnerability.
6965565	Exception thrown in `catalina.out` when logging in or out of the Administration Console.
6966338	`tarantella security enable` command with a Thawte test certificate fails to accept root or intermediate certificate.
6966795	Secondary server needs to be restarted to pick up bean property changes.
6966878	Search filter change is not used globally.
6966937	SGD has two connections to domain controller and global catalog.
6967576	JavaScript disabled warning message improperly aligned.
6967749	Entering new password that is too short does not let you enter another new password.

Reference	Description
6967860	`tarantella status` command shows `unable to convert date-time string` error.
6968337	PDF printing fails on Solaris OS Trusted Extensions. GPDF reports the file is damaged or does not seem to exist.
6968598	Bad behavior with multi-screen Mac OS X and Sparc server (piano).
6968772	Keymaps: Windows client and Swiss German keyboard.
6969040	Shadowing does not work.
6969452	Clicking 'Return' after entering password does not attempt login.
6969904	Cannot load-balancing JSP to work.
6970530	SGD should work with SELinux in enforcing mode.
6970615	`securid.exp` needs updating to support SecurID PAM agents.
6970836	Issues with third-party authentication and LDAP.
6970897	"Logged Out" page has no login button.
6970935	Dead key and space key behavior not correct for Windows client and UNIX applications.
6971668	Unable to launch applications on unknown Linux application servers.
6973527	Printing from Widows Server 2008 r2 using MS Publisher imagesetter driver and Solaris OS default Ghostscript version causes "`error, job success`".
6974160	SGD Enhancement Module installer does not add necessary registry keys.
6974420	Error when trying to resume an application across the array.
6974458	Windows desktop does not display correctly on Mac clients.
6974473	SGD Client crashes after resuming to a different browser on same client when saving data to mapped drive.
6974537	SGD has issues with Japanese Hankaku, Zenkaku and Kanji keys on UNIX clients.
6974820	Alt text on the Login page is not localized.
6974978	Pasting from local Linux (Ubuntu) to remote Solaris OS crashes `gedit`.
6975315	SGD Enhancement Module install dialog is not as pretty as it might be
6975665	Axis services list page reports an error.
6976202	Keyboard map for X applications cannot be unlocked in the Administration Console.

5. Bug Fixes in Version 4.50

The following table lists the additional bugs that are fixed in the 4.50.933 release.

Table 3.4. Bugs Fixed in the 4.50.933 Release

Reference	Description
6690758	Mac client keyboard combinations not sent to Windows 2003 application.
6806240	Active Directory authentication, issues when configuring using the Administration Console.
6842496	Keyboard input issues in kiosk mode for Max OS X 10.5.7.
6842532	Kiosk mode issues for Mac OS X.
6849891	Upgrade causes `tarantella start` to fail.

Reference	Description
6870510	Empty LDAP groups not found for searches using Administration Console.
6872934	SGD Client does not start on non-Java clients running Japanese versions of Windows.
6874184	Active Directory authentication fails when user name includes umlaut characters.
6879788	Invalid credentials errors when using Active Directory authentication.
6890490	Seamless windows applications fail on KDE.
6890996	Intermittent array stability issues.
6893011	Apache web server security vulnerabilities.
6893767	Audio issues for Remote Desktop Connection applications.
6898102	Password cache issue with JDK 6u16.

The following table lists the significant bugs that are fixed in the 4.50.907 release.

Table 3.5. Bugs Fixed in the 4.50.907 Release

Reference	Description
6357003	Native client cannot launch browser on Solaris.
6574482	Update Kerberos to version 1.6.1.
6598774	TEM download page only refers to Windows 2003 and Windows 2000 servers.
6600671	Audit logging does not show who made changes to SGD configuration.
6616090	SGD servers show fatal errors.
6616750	Preferred language is ignored when using load-balancing JSP technology page.
6620262	Login theme attribute is still available on the command line.
6621444	Issues with Portuguese Brazilian ABNT2 X keymap.
6623676	Changing the primary server takes longer than expected using the Administration Console.
6629773	Administration Console reports error and exits when browsing LDAP.
6630326	`ldapconn` and `ldapconn-lookup` cache threads are not shut down correctly after use.
6631617	Array operations need to be faster and more resilient.
6634621	Certificate validation mechanism does not explore all possible certificate paths.
6655169	Expired password cannot be changed for some application servers using authentication dialog.
6664607	Detached offline secondary does not update to standalone when brought back to the array.
6664789	Some array members have an incorrect license count after a remaster.
6665303	`tarantella status` command reports incorrect session count.
6667697	Double-byte group name causes HTTP 500 error.
6670924	Offline secondary server is detached when brought back to the array after a `make_primary` operation.
6677639	Welcome page modules link issues when Japanese language selected.
6682124	Flushing cached LDAP configuration using `tarantella cache --flush` command does not work.
6684256	Session refresh issue for objects with Japanese names.

Reference	Description
6690579	Load balancing issues mean applications will not start and SGD cannot create new user sessions.
6695309	Remove internal DNS names for cookies and tokens passed to client from SGD Gateway.
6696945	Administration Console labels not updated when changing browser language.
6700455	Load Management column is present in Licenses table.
6706081	SGD server warningerror logs are sent to standard error output.
6707889	Administration Console fails during array join for an SGD server that is disconnected from the network
6707912	Administration Console issues after detaching secondary from an array.
6708340	Ghostscript test file `sample.pdf` in `var/log` directory instead of `var/info`.
6708972	Warning message for silent shadowing is truncated.
6709596	SGD server object should be created using server name provided during install.
6710929	`xfrenchcanadian.txt` keymap is not loaded while starting SGD applications.
6711024	No audio output from Windows 2003 server application for SLES 9 Sun Ray client.
6712191	Missing default realm in `krb5.conf` file causes Active Directory integration problems.
6712756	Connections to a down server on Solaris cause long delays in array operations.
6712821	Czech QWERTY keyboards: Issues with S caron in Windows applications.
6713230	Auto-switching keyboards for Sun Ray client devices.
6713241	F11 key presses are ignored on Japanese installation.
6713366	Some translations missing from localized `SOAPResources.properties` files.
6714419	Poor usability when shadowing a low bandwidth connection.
6714906	SGD Gateway web server incorrectly determines HTTP protocol for client entry point.
6715694	Active Directory authentication takes a long time or times out.
6716562	`tarantella cache --flush krb5config` command fails if using Active Directory client certificates with no LDAP credentials in password cache.
6716771	Client printers not created on Windows 2008 server when connecting from UNIX clients.
6717020	Spool file is not deleted immediately after using PDF printing.
6718248	Issues with user-renamed PDF printers.
6720092	Timezone redirection issues with Windows applications.
6720778	`ttaexecpe` process generates core files during array scalability testing.
6721163	Enhancement Module download page only refers to Windows 2000/2003 server.
6721683	Localized help links remain on webtop after an upgrade, but point to invalid targets.
6723117	Active Directory integration does not recognize a Global Catalog host as being the same as a Domain Controller host.
6724489	My Desktop connection status message is not localized.
6724911	Issues when creating new applications with Kanji names using the Administration Console.
6725323	Unable to launch multi-byte named application from Start menu when using Integrated mode.

Reference	Description
6725479	SGD Client does not dock in the icon tray.
6725495	Mac OS X clients: Caps Lock key not synchronized correctly.
6725847	Unable to run Windows applications using Fedora Core 8 SGD server.
6725890	Array join failure using Administration Console on secondary server.
6727951	Hangul/English toggle key on Korean keyboard fails to toggle input correctly.
6728903	Application sessions for anonymous and shared users are orphaned on SGD server restart.
6729370	Querying Domain Controllers for user information should be disabled by default.
6729727	CWM windows on CDE desktop client minimize and move off screen.
6729916	Delivering server-side events via an SGD web server-JServer connection.
6730044	Administration Console fails for Active Directory LDAP searches with Chinese characters.
6730384	Primary SGD server failed on repeated login-logout tests.
6731391	If LDAP server fails, all SGD user sessions are terminated.
6732007	SecurID server list cache thread on the SGD server is not killed.
6732158	SGD Client exits after a window is closed from Quick Test Pro.
6734004	Users with Portuguese characters in Active Directory common name lose sessions periodically.
6734801	Client's Maximum Size is not calculated correctly on Linux desktops.
6734852	LDAP call always result in cache miss when missing attributes are requested.
6734906	Apache `error_log` file contains lots of "Network is unreachable" messages.
6736670	Windows application becomes unresponsive whilst scrolling.
6737141	Null pointer exception on login for users with 8-bit character in ENS name.
6738055	LDAP error logging can be uninformative and misleading.
6738069	Caught exception from `adminSearchSession` SOAP method.
6741559	Copy and paste problems with some Solaris 8 based OpenWindows binaries.
6741912	Administration Console fails to find non top-level LDAP objects without a base DN and a namingContexts attribute.
6742027	Installation of SGD appears to hang.
6742916	Issues with routing token redirection for Session Directory.
6744667	Web services client applications need to specify an IP address when using the SGD Gateway.
6744683	Window minimize issues for Borland applications displayed in seamless mode.
6745306	Windows + Tab key combination not working correctly in kiosk mode.
6746165	SGD Gateway RPM install on SUSE fails with dependency errors.
6747873	Intermittent Active Directory LDAP authentication failures.
6748390	Expired CA's cause security warnings even when another valid CA exists.
6748744	Active Directory site discovery creates alarms that are dereferenced and never cancelled.
6749795	Null pointer exception in SGD log after logging out.
6750824	Web service optimizations and bug fixes.

Reference	Description
6751874	Support multiple SKID keys for ASAD and SOAP connections to and from the SGD server.
6752431	Zombie process will not go away until SGD is restarted.
6754059	All other SGD applications are terminated when an application generates an event.
6754667	Adding an array member and removing another results in blocked threads.
6755152	Multiple Java null pointer exceptions in log files.
6755153	Webtop shows incorrect state for applications that are not resumable.
6755238	SOAP fault shown when logging out of My Desktop.
6755548	Option to resume printer state in My Desktop.
6756523	Client Window Management application issues after upgrading to JDK 1.6.
6756705	SGD Client does not run on OpenSolaris 2008.05.
6756755	`ttarandom` error messages shown in terminal window.
6757351	`tarantella security enable` command fails and deletes the private key.
6757757	Client Window Management dialogs do not stay above parent windows.
6757813	Active Directory password expiry only works if the system `krb5.conf` file is configured.
6761804	Login button on the log out splash screen is disabled.
6763485	Default window coordinates are inconsistent when using Client's Maximum Size attribute for Independent Window window type.
6763877	Mac OS 10.5.5 users unable to start SGD Client due to X11 changes in OS updates.
6765600	Proxy provider errors when logging in to SGD.
6765940	Unable to print when Active Directory user name includes German umlaut character.
6766896	Array members detached from array.
6767773	Secure Apache `httpd.conf` configuration file needed for SGD.
6767845	Multiple LDAP servers do not work as expected on LDAP server failover.
6767846	Exception thrown when using invalid search string in LDAP Directory Service Integration assignments.
6767847	Error messages seen in log files when using eDirectory with SGD.
6767848	LDAP groups not searchable when using eDirectory with SGD.
6767849	SGD does not prompt for password change after LDAP password expiry.
6769028	SGD Client does not autostart on desktop login to Solaris 10 x86.
6769538	Shadowing fails on Red Hat Enterprise Linux 5.1.
6770071	Issues when changing peer DNS name of an SGD server.
6771177	Power failure on Windows application server causes SGD Windows applications to freeze.
6774869	`tarantella security enable` command throws `retcode` error.
6776988	Administration Console fails if LDAP structure is changed from that used in an SGD LDAP search.
6777016	Active Directory and LDAP configuration settings are not replicated correctly.
6780540	LDAP operations result in unnecessary InterruptedNamingException messages.

Reference	Description
6780772	SGD server hangs when not using FQDN and trying to login with Integrated Client.
6783263	Input language switching issues for Windows applications when 3-letter code is used.
6784049	Aged password handler issues with SLES 10 application server.
6785563	SGD Client starts the wrong browser for logging in using Integrated mode.
6786285	Slow application launch due to port conflicts.
6786834	MyDesktop object not created for a Gnome desktop on SUSE 10.0.
6789743	Resuming printing for My Desktop application.
6790513	More detailed information when an array is in an inconsistent state.
6790936	Terminal type not being set when starting character applications.
6791016	Improvements for audit logging.
6791507	Killing browser generates an invalid session cookie error.
6792195	Users unable to launch applications in an array after sudden loss of a node.
6793043	Unable to lock XPE reliably using `ttatsc` on SGD 4.41.
6793493	Korean/English and Hanja keys of Korean PC keyboard do not work on Solaris client.
6793569	Array join using host short name fails and does not replicate licenses correctly.
6793749	VT420 emulator does not render some graphics characters correctly on OpenSolaris.
6794082	Korean/English and Hanja keys do not work on Solaris client.
6794618	Cross frame scripting vulnerability.
6794839	Accent characters not reproduced correctly for German locale.
6795598	`ttatdm.exe` process causes high CPU usage on the application server.
6796137	Corruption when resizing CWM windows on Ubuntu 8.10.
6796636	Extra space added after typing “^” and “~” in a Japanese environment.
6797226	Administration Console result tables do not render correctly on Internet Explorer 7.
6797638	Cannot log into Active Directory server after a period of time
6798637	SGD Terminal Services Client on UNIX platforms fails to get a licence from Windows 2008 servers, but still connects.
6798689	tarantella security disable command removes CA certificate file.
6800499	Japanese Kana mode does not work with Xsun.
6800609	SGD Client dialog box font issue.
6801579	Windows SGD Client cannot enable Kana mode for Solaris applications.
6801662	Connecting via the SGD Gateway displays an Error Page message.
6802223	Message dialog for the SGD Client Helper does not have Sun branding or localization.
6802466	`ttaxpe` repeatedly maps and unmaps client devices.
6802468	Horizontal mouse scrolling hangs emulator session on Mac OS X.
6802869	SWM applications lock up OpenSolaris desktop.
6802907	`ttaxpe` crashes when running Administration Console on SPARC Solaris.
6804663	Alternative PDF viewer setting is not saved when using the SGD Gateway.
6804665	Add Evince to default list of PDF viewers for improved out of the box support for Ubuntu.

Reference	Description
6805205	Comma on Numpad on German keyboard does not work in Windows session.
6807562	CWM windows z-order issue with Solaris clients.
6809756	Some Chinese and Taiwanese localized strings are not displayed in the Connection Progress dialog.
6810518	Default My Desktop application does not exit when you log out on Red Hat 5.1.
6811627	Expect script update for Smart Card Input Method (SCIM) on SUSE 10.
6811796	`egrep` syntax error when checking ssh X11 forwarding flag during SGD installation.
6813543	`tarantella array` command usage message wraps incorrectly on 80-character terminals.

6. Documentation Issues in Version 4.60

This section lists the known documentation issues for the 4.60 release.

6.1. Default Printer for UNIX, Linux, and Mac OS X Platform Client Devices

The published documentation incorrectly states that the default printer driver used when printing from a Microsoft Windows application server to a client printer attached to a UNIX, Linux, or Mac OS X client device is `QMS 1060 Print System`.

The default printer driver is `HP Color LaserJet 2800 Series PS`.

On page 243 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, the information about the `default.printerinfo.txt` configuration file should read as follows:

When SGD is first installed, the `default.printerinfo.txt` file contains the following entry:

```
[UNIX]
"_Default" = "HP Color LaserJet 2800 Series PS" PostScript
```

With this configuration, when users print from a Windows application server, they see a printer called `_Default`. This printer prints to the default printer on the client using a basic PostScript printer driver, "HP Color LaserJet 2800 Series PS".

6.2. Client Profile Setting for Spanning Multiple Monitors

The released documentation does not include full details for the Span Multiple Monitors (Kiosk Mode) client profile setting.

On page 193 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, add the following note to the section on “Configuring Desktop Size for Kiosk Mode Applications”.

Note

The desktop size for kiosk mode applications can also be configured from the webtop. Use the Span Multiple Monitors (Kiosk Mode) option in the Client Settings tab.

On page 317 of the *Oracle Secure Global Desktop 4.6 Administration Guide* and page 43 of the *Oracle Secure Global Desktop 4.6 User Guide*, add the following entry to the table of client profile settings.

Setting	Description
Span Multiple Monitors (Kiosk Mode)	Enables X applications to be displayed in kiosk mode on a multihead or dual head monitor. When enabled, the kiosk mode display is spanned across all monitors. When disabled, the kiosk mode display is displayed using the primary monitor only. This is the default setting.

In the “Using Multihead or Dual Head Monitors” section on page 193 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, replace the following paragraphs in the “Configuring Desktop Size for Kiosk Mode Applications” section.

“X applications can be displayed in kiosk mode on a multihead or dual head monitor.

You configure kiosk mode display features with the `<KioskArea>` entry in the `<localsettings>` section of the client profile, `profile.xml` on the client device. If the `<localsettings>` section is not present in the client profile, create a new section.

The `<KioskArea>` entry defines the screen area used by kiosk mode. The available values are as follows:

- virtual – Uses the virtual screen size. All monitors are used.
- `0` – Uses the primary monitor only. This is the default value.
- `1` – Uses the secondary monitor only.
- *n* – (Multihead monitors only). Uses the *nth* secondary monitor only.

For example, to span the kiosk mode display across all monitors:”

```
<KioskArea>virtual</KioskArea>
```

6.3. Correction to the “Array Resilience” Section

The following paragraph in the “Recovery Stage” section on page 340 of the *Oracle Secure Global Desktop 4.6 Administration Guide* is incorrect.

“If an array splits into more than two arrays during the failover stage, the original array formation cannot be recreated automatically. Manual recovery must be used.”

The paragraph should read as follows:

“If an array splits into more than two arrays during the failover stage and the Action When Failover Ends (`--array-primaryreturnaction`) attribute is configured as Restore original primary (`accept`), the original array formation is recreated automatically.

If the Action When Failover Ends attribute is configured as Restore array with a new primary (`acceptsecondary`), the original array formation cannot be recreated automatically. Manual recovery must be used.”

6.4. Correction to the “Dynamic Launch” Section

On page 170 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, the path to the `sgd-webservices.jar` file is incorrect.

The correct path is as follows:

`/opt/tarantella/bin/java/com/sco/tta/soap/services/proxy`.

6.5. Editing a List of Attributes From the Command Line

The released documentation contains inaccurate information about editing a list of attributes from the command line.

In the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide*:

- On page 59, the paragraph should read as follows:

  “Separate multiple *`filter-spec`* entries with a comma, and enclose the entire string in double quotation marks (`""`).”

- On page 60, the example for configuring multiple connection filters should read as follows:

```
"192.168.0.250:sgdg:gateway1.example.com:443,\
 *:direct:sgd1.example.com:80"
```

In the *Oracle Secure Global Desktop 4.6 Administration Guide*:

- On page 5, the example of external DNS names configuration should read as follows:

```
$ tarantella config edit --server-dns-external \
"192.168.10.*:boston.example.com" "*:www.example.com"
```

- On page 12, the example of array routes configuration should read as follows:

```
"192.168.5.*:CTDIRECT" \
"192.168.10.*:CTSOCKS:taurus.example.com:8080" \
"*:CTSOCKS:draco.example.com:8080:ssl"
```

- On page 13, the paragraph describing how to configure multiple filters in an array route should read as follows:

  “Separate each filter with a space and enclose in double quotation marks (`""`). For example, `"filter1" "filter2" "filter3"`.”

- On page 391 in the Log Filters section, the paragraph should read as follows:

  “Separate multiple *`filter`* entries with a space and enclose each filter in double quotation marks (`""`).”

- On page 496 in the External DNS Names section, the sentence at the end of the Usage paragraph should read as follows:

  “Separate multiple DNS names with a space and enclose each DNS name in double quotation marks (`""`) .”

  On the same page, the example of external DNS names configuration should read as follows:

```
--server-dns-external "192.168.10.*:boston.indigo-insurance.com" "*:www.indigo-insurance.com"
```

6.6. Incorrect Documentation URL and Customer Feedback Email Address

Following the closure of the Sun documentation site (`docs.sun.com`), the released documentation contains incorrect documentation URL and customer feedback email address details.

The documentation URL should read as follows:

`http://download.oracle.com/docs/cd/E19351-01/index.html`

The email address for customer comments should read as follows:

`VIRT-DOCS-EXT_WW@ORACLE.COM`

This change affects the following documentation:

- Oracle Secure Global Desktop 4.6 Administration Guide
- Oracle Secure Global Desktop 4.6 Installation Guide
- Oracle Secure Global Desktop 4.6 User Guide
- Oracle Secure Global Desktop 4.6 Gateway Administration Guide
- Oracle Secure Global Desktop 4.6 Platform Support and Release Notes

6.7. Deprecated --force Option Included in the Documentation

Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide* incorrectly lists the `--force` option for the `tarantella stop` and `tarantella restart` commands.

The `--force` option was deprecated in the 4.6 release and is no longer available.

6.8. Correction to the “SGD Remote Desktop Client” Section

The table of command options for the SGD Remote Desktop Client on page 152 of the *Oracle Secure Global Desktop 4.6 Administration Guide* incorrectly states that the default setting for the `-windowskey` option is `on`.

The default setting for the `-windowskey` option is `off`.

6.9. Avoiding Port Conflicts for the X Protocol Engine

The following applications troubleshooting topic is missing from the released documentation.

Application startup can take longer than expected if SGD attempts to use an X display port that is being used by another service. Application startup eventually completes successfully.

The solution is to exclude the port from use by the X Protocol Engine.

In the Administration Console, go to the Protocol Engines, X tab for each SGD server in the array and type `-xport` *`portnum`* in the Command-Line Arguments field, where *`portnum`* is the TCP port number to exclude.

Alternatively, use the following command:

```
$ tarantella config edit --xpe-args "-xport portnum"
```

To exclude several ports, you can specify `-xport` *`portnum`* multiple times, as follows:

```
$ tarantella config edit \
--xpe-args "-xport portnum_1" "-xport portnum_2" "-xport portnum_3"
```

The changes made take effect for new X Protocol Engines only. Existing X Protocol Engines are not affected.

6.10. Correction to --suffix-mappings Option Documentation

The `--suffix-mappings` option for the `tarantella service` command is incorrectly documented.

In the tables of command options on page 820 and page 825 in Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide*, the following paragraph is incorrect:

“Applies only to Active Directory service objects.”

This paragraph should read as follows:

“Applies to Active Directory service objects and LDAP service objects that connect to Active Directory.”

The initial sentence in the “Suffix Mappings” section on page 98 in Chapter 2 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, should read as follows:

“The following information applies to Active Directory service objects and LDAP service objects that connect to Active Directory.”

6.11. Correction for tarantella object new_windowsapp Command

In this release, the Window Manager (`--winmgr`) attribute is not available when you create a new Windows application object using the `tarantella object new_windowsapp` command.

The documentation for the `tarantella object new_windowsapp` command on page 744 in Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide* incorrectly lists the `--winmgr` attribute.

6.12. Documentation for tarantella config reload Command

Details for the `tarantella config reload` command are missing from the released documentation.

The following information should be included in the “The `tarantella config` Command” section on page 688 in Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide*.

tarantella config reload

Reloads properties for the server where the command is run.

Syntax

```
tarantella config reload [ --login-beans ]
```

Description

The following table shows the available options for this command.

Option	Description
`--login-beans`	Reloads server properties related to authentication, such as `com.sco.tta.server.login.DSLoginFilter.properties`. This option can be used to reload properties on a secondary server, without restarting the server.

Examples

The following example reloads all authentication properties for the server where the command is run.

```
$ tarantella config reload --login-beans
```

6.13. Correction for the Windows Audio Sound Quality Attribute

The documentation for the Windows Audio Sound Quality (`--array-audio-quality`) attribute on page 468 in Appendix A of the *Oracle Secure Global Desktop 4.6 Administration Guide* is incorrect.

The description of the High Quality Audio setting should read as follows:

- **High Quality Audio –** 44.1 kHz.

The following paragraph is missing from the Description section on the same page:

“If the application server hosting the Windows application does not support the High Quality Audio setting, the audio rate is downgraded automatically.”

6.14. Correction to “Upgrading the SGD Gateway”

The following sentence in the “Upgrading the SGD Gateway” section on page 5 of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* is incorrect.

“When you upgrade the SGD Gateway, your original configuration, such as keystores and routing proxy configuration files are preserved. There is no need to reconfigure the SGD Gateway after upgrading.”

This sentence should read as follows:

“When you upgrade the SGD Gateway, most of your original configuration, such as routing proxy configuration files is preserved. However, the upgrade process overwrites any self-signed certificates used by the Gateway.

After an upgrade, you must reconfigure the SGD Gateway. Follow the standard configuration steps for authorizing a Gateway to SGD, as described in “How to Install SGD Gateway Certificates on the SGD Array” on page 16.”

See Section 1.17, “6963320 – Cannot Connect to SGD Using Version 4.5 of the SGD Gateway, or Using an Upgraded Version 4.6 Gateway” for more details about reconfiguring the SGD Gateway following an upgrade.

6.15. Correction to Printing Troubleshooting Topic

The following sentence is missing from the “For PDF Printing, is Ghostscript Available on the SGD Host?” printing troubleshooting topic on page 250 in Chapter 5 of the *Oracle Secure Global Desktop 4.6 Administration Guide*.

“Try upgrading to the latest version of Ghostscript. After upgrading, ensure that the symbolic link `/opt/tarantella/var/info/gsbindir` points to the directory where the new Ghostscript binaries are installed.”